Criteri da utilizzare per individuare, ai fini dell'accertamento di cui all'art. 11, comma 2, del decreto legislativo 6 settembre 1989 n. 322, le unità di rilevazione la cui mancata risposta comporta l'applicazione della sanzione amministrativa di cui all'articolo 7 del d.lgs. n. 322/1989 (art. 13 comma 3-ter d.lgs. n. 322/1989)
e correlato
Elenco dei lavori (Sdi e Sda) compresi nel *Psn 2020-2022* per i quali la mancata fornitura dei dati configura violazione dell'obbligo di risposta - Anno 2020

Programma statistico nazionale 2020-2022

Criteri da utilizzare per individuare le unità di rilevazione la cui mancata risposta comporta l'applicazione della sanzione amministrativa di cui all'articolo 7 del d.lgs. n. 322/1989.

Premessa

L'art. 13 del d.lgs. n. 322/1989 dispone l'emanazione di un unico provvedimento, nella forma del decreto, per l'adozione degli atti di programmazione della statistica ufficiale cui sono allegati, pertanto:

- il Programma statistico nazionale (art. 13, comma 3);

- l'Elenco delle rilevazioni rientranti nel Programma statistico nazionale che comportano obbligo di risposta da parte dei soggetti privati a norma dell'art. 7 del decreto legislativo 6 settembre 1989, n. 322 (art. 13, comma 3-ter);

- il documento contenente la definizione dei criteri da utilizzare per individuare, ai fini dell'accertamento di cui all'art. 11, comma 2, del decreto legislativo 6 settembre 1989 n. 322, le unità di rilevazione la cui mancata risposta comporta l'applicazione della sanzione amministrativa di cui all'articolo 7 del medesimo decreto (art. 13 comma 3-ter).

Il presente documento, in ottemperanza a quanto previsto dalla normativa vigente, reca la definizione dei criteri da utilizzare per individuare, ai fini dell'accertamento di cui all'art. 11 comma 2 del d.lgs. n. 322/1989 e s.m.i., le unità di rilevazione la cui mancata risposta comporta l'applicazione della sanzione amministrativa di cui all'articolo 7 e il correlato Elenco di lavori compresi nel Psn 2020-2022 per i quali la mancata fornitura dei dati configura violazione dell'obbligo di risposta .

La selezione annuale delle rilevazioni relativamente alle quali la mancata fornitura dei dati configura violazione dell'obbligo di risposta ai sensi del primo comma dell'art. 7 del d.lgs. n. 322/1989 sarà condotta tra quelle assoggettate a tale obbligo in quanto contenute nel Psn e, per i soggetti privati, nell'apposito elenco di cui al decreto legislativo 6 settembre 1989 n. 322, art. 13, comma 3-ter.

La selezione deve comunque garantire il coinvolgimento equilibrato dei diversi soggetti del Sistan titolari delle rilevazioni.

Con riferimento ai lavori per i quali l'applicabilità della sanzione ai soggetti inadempienti è subordinata al possesso di specifiche caratteristiche delle unità statistiche (valori soglia), le variabili di riferimento e i relativi valori soglia sono esplicitati nell'elenco delle indagini selezionate. I dati utilizzati per verificare la sussistenza delle suddette caratteristiche sono quelli contenuti nei registri nella disponibilità del titolare. Tali dati, validati prima dell'avvio dell'indagine dal titolare del registro con apposito provvedimento di cui è resa notizia sul sito istituzionale, sono accessibili esclusivamente ai diretti interessati in conformità alle regole previste dalla normativa vigente e con le modalità indicate in occasione dell'avvio dell'indagine.

Con riferimento alle rilevazioni congiunturali - ognuna da considerare come un'unica indagine - caratterizzate da una pluralità di forniture nel periodo di riferimento, ai fini dell'applicazione delle sanzioni amministrative di cui agli artt.7 e 11 del d.lgs 322/1989 e s.m.i., si configura come:

- "Omessa" la fornitura di dati non pervenuta o pervenuta oltre il termine di conclusione dell'indagine;
- "Incompleta" la fornitura parziale o trasmessa oltre gli specifici termini stabiliti dal Titolare, in coerenza con la metodologia elaborata per ciascuna indagine.

Principi generali

Le raccomandazioni europee e internazionali specificano che le amministrazioni, le imprese e le famiglie nonché il pubblico in generale possono essere obbligati dalla legge a fornire dati su richiesta delle autorità statistiche. L'obbligo di risposta ha l'obiettivo soprattutto di "certificare" la serietà e l'ufficialità della rilevazione e di far comprendere ai rispondenti l'importanza della rilevazione statistica che si sta effettuando e, quindi, di favorire l'ottenimento delle risposte da parte delle autorità statistiche che, a tal fine, sollecitano il rispondente a fornire la risposta. Si tratta di una sorta di *"mandato per la rilevazione dei dati"* (principio numero 2 del Codice delle statistiche europee), cioè di una leva da usare per facilitare l'attività della statistica ufficiale.
In caso di rifiuto di risposta può essere stabilito un sistema di sanzioni nei riguardi dei non rispondenti al fine di certificare l'importanza della rilevazione e di avere un "effetto educativo" per coloro che si rifiutano di rispondere.
Come risulta dal suddetto codice e dai vari documenti internazionali sulla Statistica ufficiale, non si tratta di un principio o di uno strumento delle procedure statistiche e non è finalizzato, se non marginalmente, a recuperare le mancate risposte e migliorare la qualità delle informazioni statistiche da produrre.
Questi principi di carattere generale devono essere tenuti presenti per definire i criteri in base ai quali selezionare le indagini sottoposte ad obbligo di risposta per le quali deve essere applicata una sanzione ai non rispondenti.

I principi in base ai quali operare sono i seguenti:

1. L'accertamento della violazione dell'obbligo di risposta e la conseguente applicazione delle sanzioni è volta a sostenere la necessaria partecipazione e collaborazione dei rispondenti alle indagini previste dal PSN, tenendo conto soprattutto del rispetto degli standard programmati di qualità delle stime prodotte.

2. Tutte le rilevazioni per le quali sussiste l'obbligo di risposta possono essere proposte per l'accertamento delle violazioni soggette a sanzione.

3. La numerosità delle unità statistiche da sottoporre all'accertamento deve essere tale da garantire la sostenibilità finanziaria ed organizzativa da parte dell'ente titolare della rilevazione.

4. La selezione annuale delle indagini è effettuata sulla base di una serie di criteri inclusivi, definiti in termini di: a) tipologie di indagine, b) caratteristiche delle unità statistiche e c) tipo di mancata fornitura della risposta.

5. I criteri inclusivi saranno applicati in modo da garantire nel tempo, almeno parzialmente, la rotazione delle indagini e delle tipologie di dati da sottoporre alla procedura di accertamento.

Criteri generali di selezione

Coerentemente con quanto stabilito dall'art. 7 comma 1 del d.lgs. n. 322/1989 e dall'art. 13 comma 3-ter del medesimo decreto, la selezione annuale verrà effettuata sulla base dei criteri riportati nel seguito.

a) Caratteristiche dell'indagine

1. Grado di rilevanza e finalità dell'indagine, valutata sulla base dell'esistenza di atti normativi europei o nazionali che ne impongano l'esecuzione o sulla base del loro collegamento con specifici obiettivi strategici del Sistema statistico nazionale (Sistan).

2. Livello di complessità della procedura di accertamento della violazione dell'obbligo di risposta in relazione alla tecnica di indagine e al tipo di processo di produzione delle informazioni statistiche.

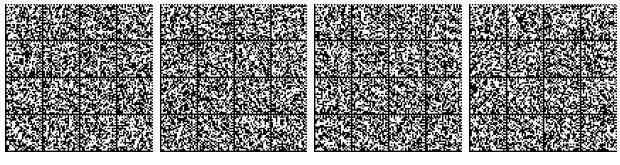
3. Dimensione del fenomeno della mancata risposta totale nelle precedenti occasioni di indagine (per le indagini periodiche) e in particolare della sua rilevanza sulla qualità delle stime prodotte.

b) Caratteristiche delle unità statistiche

1. Tipologia di unità statistica di riferimento: individui, famiglie, imprese, istituzioni, altra.
2. Dimensione e altri caratteri strutturali delle unità di rilevazione.

c) Caratteristiche delle mancate risposte

1. Reiterazione nel tempo della mancata fornitura delle informazioni richieste. Tale criterio potrà trovare applicazione con riferimento alle indagini periodiche.



Elenco dei lavori (Sdi e Sda) compresi nel Psn 2020-2022 per i quali la mancata fornitura dei dati configura violazione dell'obbligo di risposta - Anno 2020

Con riferimento ai lavori per i quali l'applicabilità della sanzione ai soggetti inadempienti è subordinata al possesso di specifiche caratteristiche delle unità statistiche (valori soglia), le variabili di riferimento e i relativi valori soglia sono esplicitati nella colonna 3 del presente elenco. I dati utilizzati per verificare la sussistenza delle suddette caratteristiche sono quelli contenuti nei registri nella disponibilità del titolare. Tali dati, validati prima dell'avvio dell'indagine dal titolare del registro con apposito provvedimento di cui è resa notizia sul sito istituzionale, sono accessibili esclusivamente ai diretti interessati in conformità alle regole previste dalla normativa vigente e con le modalità indicate in occasione dell'avvio dell'indagine.

Codice	Denominazione	Soggetti sanzionabili
IST-00050	Rilevazione sull'occupazione, orari di lavoro, retribuzioni e costo del lavoro nelle grandi imprese	Tutte le imprese appartenenti alla rilevazione
IST-00066	Rilevazione statistica sull'innovazione nelle imprese	Imprese con 250 addetti e oltre
IST-00070	Rilevazione annuale della produzione industriale (Prodcom)	Imprese industriali con 250 addetti e oltre
IST-00089	Interruzioni volontarie della gravidanza	Strutture sanitarie pubbliche o private che effettuano interruzioni volontarie di gravidanza
IST-00107	Rilevazione dei prezzi di beni e servizi per il calcolo delle parità internazionali di potere acquisto (Ppa)	Imprese con 100 addetti e oltre
IST-00111	Spedizioni e arrivi di beni con i paesi UE (sistema Intrastat)	Operatori che hanno effettuato nel mese di riferimento spedizioni o arrivi per un ammontare pari o superiore a 750.000 euro
IST-00138	Capacità degli esercizi ricettivi	Regioni, Province autonome
IST-00146	Trasporto merci su strada	Imprese con 250 addetti e oltre
IST-00151	Rilevazione mensile delle vendite al dettaglio	Imprese con 100 addetti e oltre o che presentano un fatturato pari o superiore a 50 milioni di euro
IST-00229	Bilanci consuntivi di regioni e province autonome	Regione o provincia autonoma
IST-00232	Bilanci consuntivi delle camere di commercio	Camera di commercio, industria, artigianato e agricoltura
IST-00233	Rilevazione dei bilanci consuntivi degli enti previdenziali	Enti previdenziali
IST-00564	Rilevazione statistica dei permessi di costruire	Comuni italiani con una popolazione residente di almeno 20 mila unità
IST-01175	Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese	Imprese con 250 addetti e oltre
IST-01203	Rilevazione sulla struttura delle retribuzioni e del costo del lavoro	Imprese e istituzioni private con 250 dipendenti e oltre; Istituzioni pubbliche con 250 dipendenti e oltre
IST-01369	Indagine mensile sulla produzione industriale	Imprese con 100 addetti e oltre o che presentano un fatturato pari o superiore a 50 milioni di euro
IST-01370	Indagine mensile su fatturato e ordinativi	Imprese con 100 addetti e oltre o che presentano un fatturato pari o superiore a 50 milioni di euro
IST-01381	Indagine trimestrale su posti vacanti ed ore lavorate (VELA)	Imprese con 100 dipendenti e oltre
IST-01675	Rilevazione statistica "rapida" dei permessi di costruire	Comuni italiani con una popolazione residente di almeno 20 mila unità
IST-01677	Rilevazione statistica sulla formazione nelle imprese	Imprese con 250 addetti e oltre

IST-01930	Rilevazione sulle attività delle imprese a controllo estero residenti in Italia	Imprese con 250 addetti e oltre
IST-01931	Rilevazione sulle attività estere delle imprese a controllo nazionale	Imprese con 250 addetti e oltre o che presentano un fatturato consolidato pari o superiore a 500 milioni di euro
IST-02042	Indagine sui prezzi relativi all'acquisto e al possesso dell'abitazione	Imprese
IST-02300	Rilevazione territoriale prezzi al consumo	Imprese con 100 addetti e oltre
IST-02301	Rilevazione centralizzata prezzi al consumo	Imprese con 100 addetti e oltre
IST-02418	Rilevazione dei prezzi all'importazione di beni e servizi	Imprese con 100 addetti e oltre o 50 milioni di fatturato e oltre
IST-02492	Rilevazione delle liste anagrafiche comunali (LAC)	Comuni
IST-02493	Sistema Integrato Censimento permanente e Indagini sociali, componente areale	Famiglie
IST-02494	Sistema Integrato Censimento permanente e Indagini sociali, componente da lista	Famiglie
IST-02538	Rilevazione di Informazioni, Dati e Documenti necessari alla Classificazione di Unità Economiche nei settori istituzionali stabiliti dal Sistema Europeo dei Conti 2010 (SEC 2010)	Imprese; istituzioni pubbliche; istituzioni private
IST-02575	Censimenti permanenti delle unità economiche - Rilevazione censuaria delle Istituzioni Pubbliche	Istituzioni pubbliche
IST-02578	Censimenti permanenti delle unità economiche - Rilevazione campionaria sulle Istituzioni Non Profit	Istituzioni non profit con almeno 3 dipendenti
IST-02586	Rilevazione campionaria di controllo della copertura di ASIA, di aggiornamento delle unità locali (IULGI) e di completamento dei registri satellite	Imprese con 250 addetti e oltre
IST-02623	Censimenti permanenti delle unità economiche - Rilevazione multiscopo qualitativa sulle imprese	Imprese con 20 addetti e oltre
IST-02630	Rilevazione del fatturato dei servizi	Imprese con 100 addetti e oltre o che presentano un fatturato pari o superiore a 50 milioni di euro
IST-02650	Rilevazione dei prezzi alla produzione dell'industria	Imprese con 100 addetti e oltre o 50 milioni di fatturato e oltre
IST-02657	Rilevazione dei prezzi al consumo tramite acquisizione degli scanner data	Imprese grande distribuzione commerciale
IST-02673	Rilevazione dei conti economici delle imprese e per l'esercizio di arti e professioni	Imprese con 250 addetti e oltre
IST-02678	Rilevazione dei prezzi alla produzione dei servizi	Imprese con 100 addetti e oltre oppure con fatturato superiore o uguale a 50 milioni di euro
IST-02683	Rilevazione sulle previsioni di spesa per R&S delle Regioni, Province autonome e delle Amministrazioni centrali dello Stato	Regioni e province autonome
IST-02698	Rilevazione statistica sulla Ricerca e sviluppo	Imprese con 250 addetti e oltre; istituzioni non profit con 20 addetti e oltre; tutte le istituzioni pubbliche
IST-02770	Rilevazione flussi intragruppo dei principali gruppi di imprese per l'implementazione dell'Action Plan SBS	Imprese con 250 addetti e oltre o che presentano un fatturato consolidato pari o superiore a 500 milioni di euro
IST-02792	Censimento generale dell'agricoltura 2020	Unità con le forme giuridiche di Società di persone, Società di capitali, Società cooperative e Consorzi di diritto privato e altre forme di cooperazione con almeno

		3 addetti
IST-02795	Censimento permanente sulle imprese: rilevazione sulla struttura dei costi delle imprese	Imprese con 20 addetti e oltre
IST-02805	Scambi con l'estero di servizi	Imprese, istituzioni pubbliche e no profit con 250 addetti e oltre
IST-02818	Rilevazione dei prezzi di beni di investimento per il calcolo delle parità internazionali di potere acquisto (Ppa)	Imprese con 100 addetti e oltre
MSE-00005	Importazione, esportazione e consumo di prodotti carboniferi	Imprese
MSE-00009	Importazione, esportazione e consumo di prodotti petroliferi	Imprese
MSE-00012	Prezzi settimanali di alcuni prodotti petroliferi	Aziende
MSE-00014	Produzione dell'industria petrolchimica	Imprese e unità locali
TER-00001	Statistica annuale della produzione e del consumo di energia elettrica in Italia	A tutti i non rispondenti
TER-00007	Produzione e utilizzo di calore da impianti di cogenerazione elettrica	A tutti i non rispondenti
TES-00021	Conto annuale delle spese di personale delle amministrazioni pubbliche (ex ECF-00003)	Istituzioni pubbliche totalmente o parzialmente inadempienti
TES-00024	Relazione allegata al Conto Annuale delle spese di personale (ex ECF-00006)	Istituzioni pubbliche totalmente o parzialmente inadempienti
TES-00034	Indagine congiunturale trimestrale delle spese del personale dei comuni, delle province e degli enti del servizio sanitario nazionale (monitoraggio trimestrale) (ex ECF-00079)	Istituzioni pubbliche totalmente o parzialmente inadempienti

Lavori statistici che trattano dati personali momentaneamente sospesi

Programma statistico nazionale 2020-2022

I lavori statistici di seguito elencati – inclusi nel volume 2 "Dati Personali" del Programma statistico nazionale 2020-2022 – sono sospesi in considerazione dei rilievi espressi dall'Autorità Garante per la protezione dei dati personali con i provvedimenti n. 271 del 9 maggio 2018, n. 29 del 13 febbraio 2020 e n. 261 del 10 dicembre 2020, tenuto altresì conto dei pareri favorevoli espressi dalla medesima Autorità con i provvedimenti n. 10 del 23 gennaio 2020, n. 39460 del 22 ottobre 2020, n. 271 del 17 dicembre 2020 e n. 261 dell'8 luglio 2021.

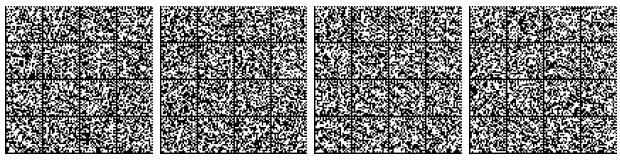
Il superamento di tali rilievi e l'avvio del trattamento dei dati personali sarà comunicato sul sito del Sistema statistico nazionale nelle pagine dedicate al Psn.

Elenco dei lavori statistici sospesi inclusi nel volume 2 "Dati personali"

ALM-00001	Razionalizzazione e valorizzazione delle Indagini sugli esiti occupazionali dei laureati, al fine di realizzare una base-dati integrata sul tema dell'istruzione universitaria
ALM-00002	Indagine AlmaLaurea sul Profilo dei Laureati
ALM-00003	Indagine Almalaurea sulla condizione occupazionale dei laureati a dieci anni dal titolo
INE-00022	IV Studio sui Consumi Alimentari in Italia (IV SCAI) - programma EU-MENU (EFSA), popolazione 10-74 anni
IAP-00019	European Social Survey
ISS-00053	Osservatorio epidemiologico sui suicidi e tentativi di suicidio
IST-02066	Indagine su Condizione e integrazione sociale dei cittadini stranieri
IST-02808	Studio delle fonti Big Data a fini statistici (ex IST-02589)

Misure tecniche e organizzative articolate per ente

Programma statistico nazionale 2020-2022



Misure tecniche e organizzative articolate per ente

Ai sensi dell'articolo 6-bis, comma1-bis, del decreto legislativo n. 322/1989, si descrivono le misure tecniche e organizzative messe in atto dai titolari del trattamento dei dati personali per attuare in modo efficace i principi di protezione dei dati degli interessati.
Il presente documento è stato predisposto sulla base delle dichiarazioni rese dagli enti titolari dei trattamenti statistici inclusi nel presente volume.

Automobile Club d'Italia

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)

L'Ente ha deliberato il proprio Organigramma Privacy ACI, che prevede gli incarichi di Referente del Trattamento, Designato e Autorizzato al Trattamento. Secondo il citato organigramma sono Referenti privacy: i Direttori/Dirigenti/Professionisti (Direzioni/Servizi/Aree Professionali) della sede centrale; i Direttori Compartimentali; i Dirigenti di Area metropolitana/Dir. territoriale; i Direttori degli Automobile Club. I professionisti statistici dell'Ente dunque sono stati nominati Referenti con specifico provvedimento.

- Interventi posti in essere per la formazione del personale: l'Ente ha previsto la formazione di tutto il Personale che a vario titolo tratta dati personali, secondo quanto indicato nella delibera del Presidente n. 7960 del 2 aprile 2019 con la quale è stato approvato l'organigramma privacy dell'ACI.

La formazione, affidata a qualificato Studio professionale si è svolta in tre moduli nel corso dell'anno 2019.

- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici

L'Automobile Club d'Italia ha predisposto un proprio Registro dei Trattamenti in ottemperanza a quanto previsto dal Regolamento EU 2016/679 (GDPR). Nel Registro dei Trattamenti ACI il trattamento riferito al lavoro PSN ACI-00013 è denominato statistiche su veicoli coinvolti in incidenti stradali e relativi intestatari Codice APSTAT_16

- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto

I professionisti dell'Area Statistica sono Attuati iscritti all'Ordine professionale e come tali rispettano un proprio Codice deontologico che prevede esplicitamente l'obbligo di riservatezza e del segreto professionale. Inoltre è garantito il riferimento alla disciplina della circolazione dei dati statistici prevista dal Codice della Statistica Ufficiale nonché l'osservanza delle regole deontologiche del Sistan
Responsabile del Trattamento dei dati è ACI Informatica, società per azioni interamente posseduta dall'Automobile Club d'Italia.

- Registrazione degli accessi delle persone nei locali n cui sono posti i server e le banche dati e la protezione degli stessi

Tale misura è prevista da ACI Informatica

MISURE TECNICHE

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Tutte le postazioni di lavoro dei dipendenti ACI sono protette da un sistema di identificazione a due fattori con password da rinnovare periodicamente. Nel 2019 tutto il personale ACI ha seguito un programma formativo volto in modo specifico alla Cyber Security

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

Tutti i sistemi elaborativi sono protetti attraverso le più moderne tecnologie di protezione perimetrale e di segmentazione di rete al fine di prevenire eventuali possibili minacce.

- Adozione di misure per garantire la qualità e la correttezza dei dati

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

i dati vengono resi anonimi al termine del trattamento e pubblicati solo in modo aggregato. Un flusso di microdati con identificativo personale (targa del veicolo) e identificativo dell'incidente (anno e numero record) viene trasmesso solo a ISTAT attraverso la piattaforma Indata.

Consorzio interuniversitario AlmaLaurea

Quanto di seguito riportato costituisce un estratto del Registro delle Attività di Trattamento.

- Modello Organizzativo e di Gestione: Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.

- Politiche e procedure per la protezione dei dati personali: La politica per la protezione dei dati personali dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Con riferimento ai singoli trattamenti, sono definite e catalogate le procedure operative e i documenti, comprese le informative e le relative modalità di somministrazione. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).

- Gestione dei Responsabili del trattamento e delle terze parti: I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.

- *Sicurezza del ciclo di vita delle applicazioni e nei progetti:* Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" introdotti dall'art. 25 del RGPD.
Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali: Nel caso si verifichino incidenti di sicurezza che comportano la "distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.
- *Gestione e formazione del personale:* Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).
- *Controllo degli accessi fisici:* Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.
- *Sicurezza dei documenti cartacei:* Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.

MISURE TECNICHE
- *Minimizzazione della quantità di dati personali:* Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
- *Partizionamento dei dati:* Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati
Cifratura
Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche.
Applicata solo nei trattamenti che riguardano categorie particolari di dati
- *Pseudonimizzazione:* Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.
Applicata solo nei trattamenti in ambito statistico
- *Controllo degli accessi logici ed autenticazione:* Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.
- *Sicurezza dell'ambiente operativo:* Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.
- *Sicurezza della rete e delle comunicazioni:* Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi degli Atenei. A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.
- *Tracciatura e monitoraggio:* Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini.
- *Gestione sicura del cambiamento:* Esistenza ed attuazione di un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata.
- *Gestione sicura dell'hardware, delle risorse e dei dispositivi:* Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.
- *Gestione sicura delle postazioni di lavoro:* Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di office automation, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software non autorizzato, accesso a siti potenzialmente pericolosi).
- *Backup e Continuità operativa:* Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.
- *Manutenzione delle apparecchiature:* Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi.
- *Protezione dalle fonti di rischio ambientali:* Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.

Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA)

A causa della diversità dei lavori statistici (rilevazioni o elaborazioni) e del dipartimento a cui afferiscono, non tutte le misure sono attuate per tutti i lavori statistici.

MISURE ORGANIZZATIVE

- Per quanto concerne l'assetto organizzativo interno all'Enea per la gestione della protezione dei dati personali e la definizione dei ruoli dei soggetti coinvolti nel trattamento, con Disposizione n. 126/2018/PRES del 14/05/2018 è stato nominato il Gruppo di lavoro per il supporto tecnico in materia di protezione dei dati personali ai sensi del Regolamento (UE) 2016/679 e della normativa generale sulla privacy nell'agenzia ENEA, composto da Referenti privacy individuati presso ogni Dipartimento/Direzione/Unità; con Disposizione n. 426/2019/PRES del 16/12/2019 è stato formalizzato l'affiancamento del gruppo da parte di uno staff tecnico-informatico; i soggetti autorizzati a trattare i dati sono individuati mediante l'appartenenza organica alla struttura di pertinenza; il DPO è stato tempestivamente nominato: fino al 3 aprile 2020, il ruolo è stato svolto da una società esterna; a far data dal 4 aprile 2020, il servizio è svolto dall'Unità UVER-DPO nell'ambito dell'Unità Ufficio degli Organi di Vertice.
- Per quanto concerne la formazione del personale, è stata avviata la somministrazione a tutto il personale di un corso e-learning sulla piattaforma ict.enea composto di due moduli, ognuno con test finale; il corso è tracciato, con individuazione di un termine per l'ultimazione; i referenti privacy si avvalgono dei corsi organizzati dalla SNA per la formazione e l'aggiornamento.
- Per quanto concerne l'adozione del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679, l'ENEA, consapevole che il registro dei trattamenti è parte integrante di un sistema di corretta gestione dei dati personali e considerato le quantità e le tipologie di dati trattati nonché la varietà e complessità delle finalità del trattamento riferite alla globalità delle Banche Dati gestite, ha optato tempestivamente per l'acquisto di una piattaforma informatica doc.suite, in riuso (art. 68 CAD), corredata di un servizio mirato a gestire il registro dei trattamenti. Tale piattaforma è implementata e monitorata dai referenti privacy e viene semestralmente aggiornata; sono state inserite apposite sezioni che costituiscono il "diario" per tracciare l'attività formativa; registrare le riunioni del gruppo di lavoro e gli audit con il dpo esterno (fino alla data del 3 aprile 2020); le richieste di esercizio dei diritti da parte degli interessati; il registro del data breach è presente in sezione dedicata.
- Per quanto riguarda il conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) agli interessati, vengono predisposte apposite informative differenziate per le pagine web gestite da ENEA, per i trattamenti svolti e per le diverse banche dati.
- In caso di contitolarità del trattamento, vengono sottoscritti dal Titolare gli accordi di contitolarità con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679; in caso che sia necessario individuare un Responsabile esterno ai sensi dell'art. 28 del Regolamento (UE) n. 206/679, si provvede alla nomina relativa secondo un modello elaborato insieme al dpo che viene comunque dettagliato ed adattato al caso specifico: i soggetti esterni così nominati sono tenuti al rispetto delle istruzioni fornite dall'ENEA.
- Per garantire l'esercizio dei diritti degli interessati, sono state attivate email dedicate privacy@enea.it e uver.dpo@enea.it, costantemente presidiate da personale appositamente formato, con la supervisione del dpo.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Vi sono diversi sistemi di autenticazione: i servizi centralizzati di ENTE prevedono una sistema di autenticazione basato su Active Directory; le credenziali sono assegnate ad ogni dipendente e/o ad ogni persona avente diritto all'accesso; la password ha un requisito minimo di complessità (8 caratteri, numeri, segni speciali) e deve essere modificata almeno una volta l'anno;
- I sistemi gestionali hanno un proprio sistema di autenticazione, solo il personale autorizzato può accedere ai relativi Data Base; la password ha un requisito minimo di complessità (8 caratteri, numeri, segni speciali) e deve essere modificata almeno due volta l'anno;
- Tutti i server che erogano servizi interni (network, security, ecc) hanno un proprio sistema di autenticazione; solo il personale ICT con qualifica "system Administrator", può accedere ai server, l'utenza è strettamente personale; la password ha un requisito minimo di complessità (8 caratteri, numeri, segni speciali) e deve essere modificata almeno una volta l'anno; rimane possibile l'uso delle credenziali Administrator/Admin/root solo per specifiche esigenze.
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di pseudonimizzazione;
- Tutta la rete ENEA è protetta da firewall perimetrali; le policy sono stabilite centralmente e predisposte sui singoli apparati. Verso l'esterno sono aperti solo i server e/o i servizi che erogano servizio ad altri enti, alla comunità scientifica o ai cittadini.

Gli utenti ENEA hanno largo accesso alla rete internet, ma sono vietati l'acceso a siti ritenuti malevoli o non legati alla attività istituzionale dell'Ente.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati;
- Alcuni server/servizi sono accessibili solo da alcune reti ENEA, altri dati medici del personale non sono in rete e vi si accede solo sulla postazione che possiede il dato.
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Tutti i server sono soggetti a backup, vengono eseguiti test periodici di restore per valutare la correttezza delle procedure;
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Anpal

MISURE ORGANIZZATIVE

- Definizione e adozione del modello organizzativo in materia di protezione dei dati personali, e conseguente individuazione dei ruoli e responsabilità dei soggetti che effettuano il trattamento, ivi incluso:
- Individuazione dei soggetti interni all'Agenzia che compiono le operazioni di trattamento, formalmente identificati mediante specifica nomina ad autorizzato del trattamento, attraverso cui i soggetti suindicati sono istruiti circa le modalità conformi per eseguire le attività di trattamento dei dati personali, ai sensi e per gli effetti dell'art. 29 del Regolamento 2016/679 (c.d. "GDPR") e dell'art. 2-quaterdecies del D.lgs. 196/2003 (c.d. "Codice della Privacy") e ss.mm.ii.;
- Individuazione dei Delegati interni, ossia dei soggetti interni ad ANPAL aventi la responsabilità di una o più Divisioni/ Strutture selezionati e preposti dal Titolare allo svolgimento di attività di monitoraggio, verifica e coordinamento in merito al trattamento dei dati personali di propria competenza;

- Identificazione e designazione del *Data Protection Officer* figura interna all'Agenzia che, tra gli altri compiti, fornisce consulenza in ambito data protection al fine di garantire il rispetto dei principi di "privacy by design & by default" e verifica l'osservanza della normativa all'interno dell'Agenzia;
- Sottoscrizione di specifici accordi sul trattamento ex art. 28 del GDPR, contenenti, tra l'altro, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, con i fornitori di beni e servizi che, nell'espletamento dei propri servizi, trattino dati per nome e per conto di ANPAL. Tali fornitori sono designati Responsabili del trattamento intesi, ai sensi dell'Art. 4 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare";
- Predisposizione del modello di Contitolarità del trattamento ex art. 26 del GDPR da sottoscrivere con i soggetti che, congiuntamente all'Agenzia, definiscono finalità e mezzi del trattamento;
- Definizione, in ottemperanza a quanto prescritto dal GDPR circa l'obbligo di ciascun Titolare di sensibilizzare e formare il personale che partecipi ai trattamenti di Dati Personali, di un Piano di formazione specifico in materia di protezione dei dati personali in cui coinvolgere tutti i soggetti interni all'Agenzia autorizzati ai singoli trattamenti;
- Definizione dei processi e relative procedure operative in termini di Data Privacy, ivi incluse:
  - procedura di gestione delle richieste degli interessati che disciplina le attività da porre in essere al fine di gestire l'esercizio dei diritti dei soggetti cui si riferiscono i dati personali trattati da ANPAL in ottemperanza al GDPR;
  - procedura di gestione delle violazioni di dati personali (cc.dd. "Data Breach"), che disciplina le attività di rilevazione, gestione, notifica e risoluzione delle eventuali violazioni di dati personali trattati da ANPAL;
  - procedura di esecuzione della valutazione d'impatto sulla protezione dei dati(c.d. "DPIA"), che descrive il processo per la realizzazione della valutazione di impatto sulla protezione dei dati, inclusi la metodologia di DPIA e i relativi tool, ai sensi dell'art. 35 del GDPR;
- Predisposizione del Registro delle attività di trattamento ai sensi dell'Art. 30 del Regolamento UE 679/2016 e definizione del processo da attuare per assicurare la tenuta, la conservazione e l'aggiornamento del Registro stesso. Il suddetto processo prevede tra l'altro, la pianificazione di controlli periodici volti a verificare l'esaustività e la correttezza del Registro delle attività di trattamento;
- Adeguamento e/o predisposizione ex novo delle informative da rendere ai soggetti interessati (e.g. beneficiari iniziative e misure di politica attiva, dipendenti, etc.) dai singoli trattamenti effettuati dall'Agenzia ex artt. 13 e successivi del GDPR.

MISURE TECNICHE

Di seguito si descrivono le misure di sicurezza tecniche definite da ANPAL ai sensi dell'art. 32 del GDPR per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture. Tali misure risultano, tra l'altro, conformi a quanto prescritto dal Provvedimento del Garante per la Protezione dei Dati Personali del 2 luglio 2015 circa "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche".
- Assegnazione dei profili di autorizzazione agli utenti sulla base del principio del "need to know" al fine di garantire che gli utenti possano accedere solo alle funzioni per le quali sono effettivamente abilitati;
- Implementazione di un processo di autenticazione basato su un sistema centralizzato di Identity and Access Management che prevede differente modalità di accesso, in base al livello di riservatezza attribuito alle informazioni (e.g. SPID livello 2 o superiore, CNS o CIE, credenziali di accesso "interne", costituite da username e password);
- Protezione da Malware tramite l'adozione e l'aggiornamento continuo di Antivirus;
- Misure di protezione sia perimetrali logico-fisiche (IntrusionPrevention System, IntrusionDetection System, ecc.) sia nei flussi di comunicazione dei dati, tramite l'implementazione di protocolli crittografici idonei a garantire la sicurezza dei dati in transito
- Implementazione di meccanismi di controllo degli accessi garantendo, tramite autenticazione, che solamente gli utenti autorizzati possano accedere ai dati e garantendo, inoltre, che i soggetti autenticati abbiano accesso solamente ai dati strettamente correlati allo svolgimento delle proprie mansioni;
- Valutazione e correzione continua delle vulnerabilità e patch management;
- Copie periodiche di sicurezza dei dati;
- Complementazione di meccanismi di cifratura e pseudonimizzazione dei dati personali trattati;
- Tracciamento log sull'utilizzo della piattaforma, log applicativi e di sistema;
- Aggiornamento continuo delle misure tecniche di sicurezza implementate;
- Definizione e implementazione di una politica per la gestione delle password "interne": la password è conservata sulla piattaforma ed ha validità di 90 giorni; la password deve avere una lunghezza minima di 8 caratteri e contenere almeno un carattere per ciascun delle seguenti tipologie:
  - Caratteri dell'alfabeto maiuscoli (A-Z)
  - Caratteri dell'alfabeto minuscoli (a-z)
  - Numeri (0-9)
  - Caratteri non alfabetici (ad esempio .,!, $, #, %).

Anpal Servizi

MISURE ORGANIZZATIVE

- Assetto organizzativo interno ad Anpal Servizi per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti neltrattamento

In ottemperanza del Regolamento UE 679/2016, Anpal Servizi ha istituito la figura del Responsabile della Protezione Dati, nominando in data 09/03/2018 Giuseppe Bartone (determinazione dell'Amministratore Unico n. 18 del 09/03/2018).
È attualmente in fase di approvazione la revisione del modello organizzativo privacy definito in coerenza con la recente riorganizzazione aziendale, che comprende l'Ufficio di Statistica istituito ex DPCM 14 febbraio 2018 e posto sotto la direzione del Responsabile la cui nomina è stata ratificata dall'Istituto Nazionale di Statistica *(doc prot. 1013132/18 del 11/06/2018).*
A tutti i lavoratori *(dipendenti e collaboratori),* nell'ambito del loro ruolo nella gestione della protezione dei dati personali, vengono impartite precise istruzioni per la gestione delle attività operative quotidiane, conformi alle regole aziendali e alle disposizioni normative privacy.

- Gestione delle autorizzazioni all'accesso ai dati
Gli autorizzati al trattamento vengono dotati di credenziali personali per l'accesso alle risorse informatiche aziendali attive per tutta la durata del loro rapporto di lavoro con Anpal Servizi. Tali credenziali vengono profilate ed aggiornate secondo la policy aziendale in modo che ogni utente possa accedere solo ed esclusivamente ai dati ed ai documenti a cui è autorizzato.
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'art. 30 del Regolamento UE 679/2016
Anpal Servizi, in qualità sia di titolare per i propri trattamenti che di responsabile verso altri soggetti, monitora regolarmente e aggiorna un proprio Registro dei trattamenti, così come previsto dall'art. 30 del Regolamento UE 679/2016.
- Interventi posti in essere per la formazione delpersonale
A tutto il personale dei Anpal Servizi *(dipendenti, collaboratori e collaboratori con il ruolo di navigator)* è stato erogato un percorso obbligatorio di formazione sul trattamento dei dati personali denominato "i principi del Regolamento UE 679/2016 e la sua applicazione nel contesto aziendale". Il corso è composto di moduli di formazione on-line corredati da materiale informativo di approfondimento e per la sua conclusione prevede l'esecuzione di un test finale per il rilascio del relativo attestato.

MISURE TECNICHE
- Sistema di autenticazione individua/e degli utenti e tracciamento degli accessi
Il personale dell'Ufficio di Statistica accede, mediante credenziali individuali, alle postazioni presenti all'interno della sala CED *(Centro Elaborazione Dati)* e quindi al server su cui sono depositate le basi dati. Tutti gli accessi sono tracciati e memorizzati in file di log.
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro
L'Ufficio di Statistica di Anpal Servizi dispone di una sala CED *(Centro Elaborazione Dati)* con accesso riservato al solo personale del suddetto ufficio, nominato con Ordine di Servizio interno N.01/2019.
- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione anche per il trattamento di categorie particolari di dati o *categoria vulnerabili di interessati*
I server *(macchine virtuali)* e le postazioni di lavoro (PC} acceduti dall'Ufficio di Statistica sono attestati su un'unica sottorete dedicata protetta mediante due firewall ridondati. I firewall implementano le regole che garantiscono l'isolamento logico della sottorete.
Anpal Servizi, attraverso il proprio Ufficio di Statistica, nell'ambito del *Programma Statistico Nazionale 2020-2022,* tratta le diverse tipologie di dati di seguito descritte:
- Microdati Sistan delle indagini Campionarie, messi a disposizione dall'Istituto Nazionale di Statistica.
- Microdati del Sistema Informativo amministrativo delle Comunicazioni Obbligatorie, messi a disposizione dagli Uffici di Statistica di Anpal e del Ministero del Lavoro e delle Politiche Sociali. I dati personali vengono forniti privi dei dati identificativi.

- Adozione di misure per garantire la qualità e la correttezza dei dati
Nell'ambito delle proprie attività l'Ufficio di Statistica adotta le misure previste dalle linee guida del *Sistan* in materia di qualità e correttezza dei dati.
Con riferimento ai progetti del PSN di cui l'Ufficio è titolare, nell'ambito dell'attività di ricerca del progetto *"Famiglie e Lavoro (ILA-00001)* sono adottate le procedure metodologiche definite dall'lstat per la ricostruzione delle variabili familiari presenti nella *Rilevazione continua sulle forze di lavoro.*
Nel caso delle attività di supporto al progetto di ricerca "*mercato del lavoro degli stranieri in Italia (LPR-00130),* la cui titolarità è in capo al Ministero del Lavoro e delle Politiche Sociali, l'ufficio di Statistica effettua l'elaborazione dei dati di natura campionaria da fonte lstat e di natura amministrativa da fonte del Ministero del Lavoro, Sistema Informativo delle Comunicazioni Obbligatorie. I dati personali, nel caso delle Comunicazioni Obbligatorie, vengono forniti dal Ministero del Lavoro e delle Politiche Sociali privi dei dati identificativi.
Nell'ambito delle attività del progetto di ricerca *"La domanda di lavoro per bacino dei Centri per l'impiego (ILA-00002),* l'ufficio di Statistica effettua l'elaborazione dei dati di natura amministrativa da fonte del Ministero del Lavoro, Sistema Informativo delle Comunicazioni Obbligatorie. I dati personali, nel caso delle Comunicazioni Obbligatorie, vengono forniti privi dei dati identificativi.

Agenzia nazionale di valutazione del sistema universitario e della ricerca - ANVUR

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati
All'interno di ANVUR le figure coinvolte nei trattamenti sono individuate sulla base dell'area organizzativa di appartenenza e del ruolo svolto.
In conformità all'art. 30 del GDPR è stato predisposto il Registro dei Trattamenti nei quali vengono specificamente individuati tutti i tipi di trattamento effettuati per i singoli ambiti di attività dell'ANVUR.
In conformità alle disposizioni in materia di trattamento dei dati personali, è stato inoltre designato il Responsabile della protezione dei dati personali, soggetto esterno rispetto all'organigramma aziendale che svolge le attività ad esso attribuite dall'art. 39 del Regolamento europeo n. 2016/679 con le garanzie di indipendenza e di autonomia previste dalle disposizioni normative vigenti.
- Gestione delle autorizzazioni all'accesso ai dati
Sulla base di una analisi dei processi e delle attività sono individuate – nell'ambito di ciascuna struttura – le persone autorizzate al trattamento dei dati, nonché i responsabili del trattamento di cui all'articolo 28 del citato Regolamento. La designazione di soggetti autorizzati nell'ambito del proprio assetto organizzativo avviene in forma scritta a firma del titolare del trattamento dei dati con la *Nomina a persona autorizzata al trattamento dei dati personali* e la relativa definizione dell'ambito di autorizzazione al trattamento dei dati stessi.
L'accesso ai sistemi informatici, e ai relativi dati personali ivi contenuti, viene configurato dal servizio dei sistemi informativi sulla base del ruolo del personale autorizzato e delle indicazioni del Responsabile dell'Area di competenza.
- Pianificazione di controlli interni periodici:
Con cadenza periodica, viene effettuato un incontro on site tra il Responsabile della protezione dei dati e i referenti ANVUR per allineamento sulle tematiche privacy e progetti che prevedono il trattamento dei dati personali.
È pianificata un'attività di verifica su base annuale al fine di valutare il livello delle misure tecniche e organizzative e definire le azioni di miglioramento necessarie.
- Adesione a codici di condotta e a meccanismi di certificazione

L'art 2-quater del Codice Privacy fa salvi i codici di condotta vigenti per i trattamenti dati ai fini statistici, cui ANVUR ha aderito. Inoltre, al fine di assicurare la tutela dei dati personali e diffondere la cultura della privacy a ciascuna persona autorizzata:
- viene consegnato il Regolamento interno con le istruzioni per il corretto trattamento dei dati personali;
- è erogata una sessione di formazione, che prevede in linea di massima i seguenti argomenti:
    - normativa di riferimento;
    - modello organizzativo, ruoli e responsabilità
    - sistema sanzionatorio
    - rischi che incombono sui dati e misure di sicurezza
    - istruzioni per il corretto trattamento dei dati personali
    - casistiche particolari nell'ambito dei trattamenti svolti da ANVUR.

- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto

In caso di trattamento dei dati svolto da soggetti esterni per conto dell'ANVUR, attraverso atti formali di designazione viene nominato un responsabile del trattamento ai sensi dell'articolo 28 del Regolamento europeo. La designazione di tali figure e l'individuazione delle relative funzioni viene formalizzata all'interno di appositi atti. I soggetti esterni designati quali *Responsabili del trattamento* sono tenuti al rispetto delle disposizioni e delle istruzioni fornite da ANVUR.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

L'accesso fisico alla sede di ANVUR è regolato attraverso: a) l'utilizzo di badge personali a tutti i dipendenti e collaboratori; b) un sistema di controllo automatizzato degli accessi; c) un servizio di vigilanza. L'accesso alle aree riservate e alla cd. "Sala CED" è autorizzato al solo personale formalmente incaricato in base al principio di necessità.

- Modalità di conferimento delle informazioni ai sensi degli articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte di ANVUR mediante informative del Titolare del Trattamento, trasmesse o consegnata direttamente, ove possibile, contenenti tutte le informazioni necessarie per il trattamento, ai sensi dell'art. 13 del Regolamento UE 2016/679,

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

Ciascun interessato può esercitare i propri diritti attraverso le modalità indicate nell'Informativa. Il Responsabile del procedimento, Il direttore, con il supporto del DPO analizzano le richieste e condividono le risposte nei termini previsti dalla normativa.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

L'accesso alle infrastrutture tecnologiche di ANVUR prevede l'utilizzo di credenziali di autenticazione individuali fornite ad ogni dipendente al momento dell'assunzione, con rinnovo obbligatorio ogni sei mesi. A breve con la migrazione in cloud, le medesime credenziali saranno utilizzate dagli utenti abilitati per l'accesso dall'esterno alla rete informatica di ANVUR tramite VPN di tipo SSL realizzata con i firewall.
L'autenticazione si basa sul principio che ogni utente che accede alle risorse del sistema deve essere univocamente identificato attraverso un codice, unico nel sistema e associato strettamente ad una persona fisica, che ne è responsabile dell'uso. La specifica risorsa informatica verifica le credenziali dell'utente e concede o meno l'accesso, tracciandolo nel sistema. L'utente può così accedere alla risorsa in base ai suoi profili di abilitazione.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

La sicurezza delle postazioni fisiche di lavoro (PC) è realizzata tramite:
- accesso attraverso le credenziali di autenticazione personali;
- impostazione dello screensaver per evitare l'accesso da parte di personale non autorizzato in caso di spostamento dalla stazione di lavoro;
- accesso controllato all'edificio (servizio di portineria centralizzato);
- accesso controllato alle stanze (dotate di serratura).

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

- ANVUR è dotato di un sistema di sicurezza perimetrale realizzato tramite firewall in configurazione HA (alta affidabilità). I firewall analizzano le richieste di accesso da/per la rete esterna ed effettuano controlli di sicurezza sul traffico della rete. I firewall effettuano inoltre un controllo del traffico di rete per la rilevazione di anomalie e tentativi di intrusione.
- nei progetti che prevedono l'utilizzo di dati individuali vengono utilizzate tecniche di pseudonimizzazione per il trattamento dei dati.

- Adozione di misure per garantire la qualità e la correttezza dei dati

La raccolta, la sincronizzazione, la conservazione e l'elaborazione dei dati avviene attraverso un sistema integrato composto da:
- flussi informativi concordati con partner informatici e istituzionali;
- software specificamente sviluppato secondo standard di sicurezza informatica.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

Le anomalie e gli incidenti aventi ripercussioni sul sistema informatico e sui livelli di sicurezza sono riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione al fine di minimizzarne l'impatto**.**

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

ANVUR effettua, con specifiche policy (frequenza e tipo di backup in relazione al grado di criticità e variabilità dei dati), i backup dei server, delle basi dati e dei repository condivisi e in uso alle diverse unità organizzative. Le intelligenze dei sistemi di memorazione utilizzati quali Storage Area Network (SAN) sono ridondate e le stesse consentono di implementare meccanismi di protezione del dato da eventuali guasti (RAID).
È in fase di predisposizione un piano di continuità operativa che permette ad Anvur di affrontare in modo organizzato ed efficiente le conseguenze di eventi imprevisti garantendo il ripristino dei servizi critici in tempi e con modalità che consentano di ridurne le conseguenze negative.
I piani di manutenzione dei server prevedono backup giornaliero con conservazione dei backup per 30 giorni.

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

In attuazione alla normativa vigente, al fine di riutilizzare, dismettere o rottamare apparecchiature elettroniche su cui siano stati memorizzati dati personali, il personale competente provvede alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino e, ove tale cancellazione non fosse realizzabile, alla distruzione del supporto. La cancellazione sicura delle informazioni è effettuata tramite la formattazione dei dispositivi. Anche in caso di riutilizzo o dismissione di pc e server su cui siano stati memorizzati dati personali, è obbligatorio provvedere alla loro preventiva cancellazione sicura in maniera da renderne inintelligibile il contenuto.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

In relazione a specifici progetti che prevedono il trasferimento di dati all'esterno sarà attivata un'area dedicata. La trasmissione di dati all'interno avviene esclusivamente attraverso rete privata previo accesso con utenza e password personali.

- Archiviazione e conservazione dei dati

i dati personali o individuali trattati da Anvur con l'ausilio di strumenti elettronici sono archiviati e conservati in file o banche dati che risiedono su server gestiti a livello centrale. Non possono essere memorizzati su aree condivise pubbliche. I server appartengono:

- alla rete privata di ANVUR;
- alle reti private dei partner informatici che offrono servizi di tipo infrastrutturale (IAAS) secondo livelli di servizio (SLA) concordati.

- Diffusione e comunicazione dei dati

È consentita la diffusione dei soli dati sui quali siano stati effettuati i necessari controlli per garantirne la rispondenza alle norme sul segreto statistico e sulla riservatezza. In ogni caso, i dati statistici prodotti possono essere diffusi solo in forma aggregata, in modo da non poter risalire all'identificazione degli interessati.

Città metropolitana di Bologna

La descrizione delle misure organizzative e tecniche adottate sono inerenti la scheda PSN PBO 00004 Sistema informativo provinciale sulla popolazione di cui è titolare la Città metropolitana di Bologna e che vede come compartecipanti tutte le Province della regione e la Regione stessa. La Regione Emilia-Romagna, raccoglie i dati dai comuni appartenenti a Province che non raccolgono autonomamente, e dalla CM di Bologna e dalle Province che raccolgono autonomamente caricando sul portale regionale i dati al termine delle procedure di controllo; la Regione adotta le misure organizzative e tecniche per il trattamento di dati personali per finalità statistiche descritte successivamente.

Si descrivono di seguito le misure tecniche e organizzative adottate dalla *Città metropolitana di Bologna.*

MISURE ORGANIZZATIVE

- L'assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento è definito nel "Regolamento metropolitano per l'attuazione delle norme in materia di protezione dati" approvato dal Consiglio metropolitano dal 14/11/2018:
(https://www.cittametropolitana.bo.it/portale/Engine/RAServeFile.php/f/NormeRegolamenti/Regolamento_Privacy.pdf)

- Gestione delle autorizzazioni all'accesso ai dati e conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto: Il Titolare del trattamento dei dati personali è la Città metropolitana di Bologna con sede in Via Zamboni, 13 - 40126 Bologna, cm.bo@cert.cittametropolitana.bo.it, nella persona del Sindaco metropolitano quale legale rappresentante dell'Ente. Ogni Dirigente è stato individuato Soggetto attuatore dei trattamenti di dati afferenti al proprio assetto organizzativo, ai sensi dell'art. 4 del Regolamento metropolitano e in forza dell'Atto del Sindaco metropolitano PG. n. 42585 del 8/07/2019 e del Decreto del Sindaco metropolitano n. 3/2020 di cui al PG. n. 11001 del 25/02/2020. Ogni Soggetto attuatore ha nominato i dipendenti dell'Ente assegnati alla struttura a lui preposta "Incaricati al trattamento" a mezzo di atto scritto. Tali provvedimenti di nomina sono stati comunicati ai destinatari e sono conservati agli atti. Nello specifico, risultano incaricati trasversalmente e impersonalmente tutti i dipendenti assegnati a tutte le strutture organizzative dell'Ente e loro articolazioni. In tal modo ogni incaricato può compiere, se del caso, operazioni di trattamento dati. In caso di trattamento dei dati svolto da soggetti esterni per conto dell'Ente, attraverso atti formali di designazione viene nominato un responsabile del trattamento la cui designazione e l'individuazione delle relative funzioni viene formalizzata all'interno di appositi atti scritti. I soggetti esterni designati quali Responsabili del trattamento sono tenuti al rispetto delle disposizioni e delle istruzioni fornite dalla Città metropolitana;

- Interventi posti in essere per la formazione del personale: al momento dell'assunzione, al personale è richiesta la frequenza obbligatoria di un corso online per la diffusione della cultura della sicurezza e della riservatezza. Il corso è obbligatorio anche per chi non risulta averlo seguito nelle diverse edizioni;

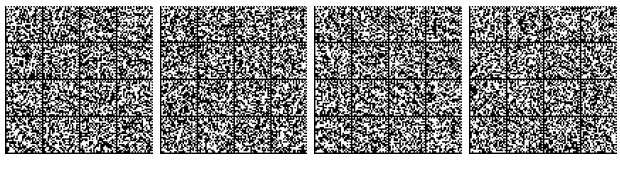
- Monitoraggio del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679 e pianificazione di controlli interni periodici: previsti ed esplicitamente richiamati all'art.10 del Regolamento metropolitano per l'attuazione delle norme in materia di protezione di dati personali, periodici controlli interni ed aggiornamenti https://www.cittametropolitana.bo.it/portale/Privacy;

- Conferimento dell'incarico di responsabile della protezione dei dati (RDP): il Responsabile esterno della protezione dei dati è Lepida S.p.A., Via della Liberazione, 15 - 40128 Bologna, dpo-team@lepida.it che ha individuato quale referente Shahin Kussai;

- Accessi ai locali in cui sono posti server e banche dati: tramite codice di accesso riservato per i soli sistemisti del Settore informatico;

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati"): nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte dell'Ente;

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati: gli interessati hanno il diritto di ottenere dalla Città metropolitana di Bologna, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza alla Città metropolitana di Bologna è presentata contattando il Titolare del trattamento dei dati o il Responsabile della protezione dei dati presso Città metropolitana di Bologna: Il Titolare del trattamento dei dati personali è la Città metropolitana di Bologna con sede in Via Zamboni, 13 - 40126 Bologna, cm.bo@cert.cittametropolitana.bo.it.



MISURE TECNICHE

- *Sistema di autenticazione individuale degli utenti, tracciamento degli accessi:* l'accesso alle infrastrutture tecnologiche dell'Ente necessita di credenziali individuali fornite ad ogni dipendente al momento dell'assunzione, con rinnovo obbligatorio richiesto in modo automatico ogni 3 mesi. La password di accesso soddisfa i requisiti attualmente in vigore (lunghezza minima 8 caratteri, mix di caratteri maiuscoli, minuscoli e speciali);
- *Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro*: l'accesso ai locali dell'Ente è consentito solo ai dipendenti che utilizzano badge personali per l'apertura dei varchi. Sono inoltre presenti telecamere di videosorveglianza e guardiole presidiate nelle sedi principali;
- *Adozione di misure per garantire la qualità e la correttezza dei dati:* sono effettuati controlli di completezza e di coerenza delle informazioni sulla base di serie storiche, rispetto e coerenza delle codifiche;
- *Adozione delle misure minime di sicurezza:* sono state adottate le misure di sicurezza come richiesto da AGID;
- *Misure di sicurezza perimetrale che allarmano in presenza di accessi fraudolenti:* I sistemi di sicurezza perimetrali sono in grado di riconoscere accessi fraudolenti e inviare messaggi di allarme;
- *Adozione di modalità di ripristino della disponibilità dei dati e dei server applicativi*: sono state definite le soluzioni tecnologiche e le modalità operative che permettono il ripristino delle funzionalità dei sistemi e di recupero dei dati;
- *Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche*: formattazione a basso livello o distruzione fisica nel caso di apparati non riutilizzabili;
- *Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni*: La trasmissione dei dati verso l'esterno viene normalmente effettuata attraverso canali sicuri. Tali tecnologie sono utilizzate all'interno solo per alcune applicazioni;
- *Adozione di sistemi di anonimizzazione* per elaborazioni statistiche interne all'Ente*:* eventuali informazioni nominative vengono eliminate al primo processo dei dati. La pubblicazione avviene solo in modo aggregato.

Si descrivono di seguito le misure tecniche e organizzative adottate dalla *Regione Emilia-Romagna*

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati);

Con la deliberazione n. 1123/20183 la Giunta regionale ha attribuito in capo al Capo di Gabinetto, ai Direttori generali, al Direttore dell'Agenzia Sanitaria e sociale regionale, al Direttore dell'Agenzia informazione e comunicazione, al dirigente competente in materia statistica precipue funzioni e responsabilità in materia di protezione dei dati personali. Con tale atto è stata operata una netta separazione delle aree di responsabilità previste in capo ai dirigenti delle strutture, funzionale alla riduzione di opportunità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione.

La sicurezza informatica, comprensiva del coordinamento sull'applicazione della normativa sulla protezione dei dati personali, è competenza del Servizio ICT Regionale che svolge l'attività anche quale strumento del Responsabile per la Transizione Digitale. A tale struttura, tra le altre cose, competono i contatti con le Autorità (come ad es. con la Polizia postale e CSIRT) e con i gruppi specialistici (ad. Es. CLUSIT). Sono state disciplinate le interazioni di tali figure con il DPO nominato.

- Gestione delle autorizzazioni all'accesso ai dati

Dipendenti e collaboratori, ai sensi dell'art. 2quaterdecies del d.lgs. 196/2003 sono autorizzati con determinazione dirigenziale, come prescritto nel modello organizzativo sopra citato.

- Interventi posti in essere per la formazione del personale

È stato di recente somministrato a tutti i dipendenti/collaboratori regionali un corso sul GDPR e sulle modalità di attuazione della normativa nell'Ente. Ogni anno viene redatto un piano della formazione del personale che viene aggiornato periodicamente con le nuove esigenze formative e viene pubblicato sulla intranet regionale.

- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici;

L'Ente ha adottato un registro dei trattamenti sin dal 2005. In questi anni il registro è stato perfezionato e arricchito di informazioni e registrazioni. È stato progettato un nuovo registro, dinamico e relazionato con altre piattaforme regionali, che andrà in produzione entro la fine del 2020.

- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto;

In caso di trattamento dei dati svolto da soggetti esterni, gli stessi sono nominati responsabili del trattamento a mezzo di uno strutturato accordo allegato al contratto. La struttura competente in materia di privacy ha prodotto e condiviso nella intranet un fac-simile cui tutte le strutture dell'ente si conformano. La nomina dei responsabili del trattamento è uno dei compiti che la Giunta ha attribuito ai Direttori generali nel modello organizzativo sopra citato.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi;

Il disciplinare tecnico regionale, approvato con la determina 1894 del 14/02/2018 ha regolamentato l'accesso alle sedi dell'Ente al fine di ridurre i rischi derivanti dall'accesso di soggetti non autorizzati alle sedi dell'Ente. Per ragioni di sicurezza, data la rilevante natura strategica e operativa del Datacenter, i locali che lo ospitano sono limitati da porte la cui apertura richiede l'utilizzo di uno specifico badge. Tali badge sono rilasciati solo previa autorizzazione. Sono attivi sistemi di allarmi e videosorveglianza. Gli accessi al datacenter sono presidiati da portineria e vigilanza.

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati");

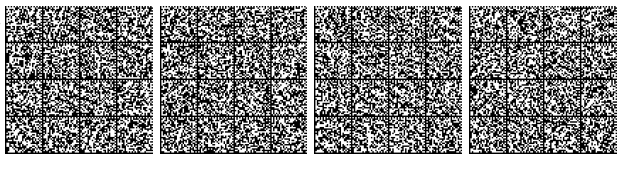
Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati attraverso apposite informative. Per le fonti di dati raccolti presso soggetti terzi, l'informativa, anche per i trattamenti con finalità statistiche, è resa all'interessato al momento dell'acquisizione del dato. L'informativa è altresì resa attraverso il Programma Statistico Nazionale in cui sono descritte le caratteristiche dei trattamenti statistici effettuati.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati;

L'Ente ha adottato con la Determina n. 14128 del 30/07/2019 un Disciplinare per l'esercizio dei diritti dell'interessato sui propri dati personali (Giunta e Assemblea), per disciplinare il workflow e le responsabilità al fine di adempiere agli oneri derivanti dalla normativa.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;



L'Ente ha implementato e formalizzato un articolato processo di provisioning per l'assegnazione o la revoca dei diritti di accesso, per le diverse tipologie di utenze e per i diversi sistemi e servizi. L'assegnazione di informazioni segrete di autenticazione è controllata attraverso un processo di gestione formale sia per utenti ordinari che per amministratori di sistema. I diritti di accesso di tutto il personale, ivi compresi i collaboratori a qualsiasi titolo, sono riesaminati a mezzo delle verifiche di sicurezza che sono effettuate a campione sulle strutture dell'Ente, oltre che su specifica segnalazione. Gli account sono, pertanto, rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, e, in ogni caso, in relazione alle modifiche intervenute nel rapporto di lavoro con l'Ente. È implementata l'autenticazione di dominio e una soluzione di Privileged Account Management.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;

Le configurazioni delle postazioni di lavoro del personale dell'Ente sono gestite in maniera centralizzata. La funzione Q0000453 è titolata responsabile di autorizzare l'installazione esclusiva dei software sulle stazioni di lavoro attraverso strumenti automatici e/o interventi da parte dei referenti informatici. In accordo alle politiche di gestione delle postazioni di lavoro, ciascun utente è tenuto a mantenere sulla propria postazione di lavoro la configurazione standard dei programmi di base e dei programmi applicativi installati e non deve interferire, impedire o ritardare la distribuzione centralizzata degli aggiornamenti del software della postazione stessa.

- Adozione di misure per garantire la qualità e la correttezza dei dati;

I lavori statistici seguono alcuni standard di qualità, come l'utilizzo di classificazioni e definizioni ufficiali o il ricorso a soluzioni metodologiche condivise per il record linkage.

Inoltre, è disponibile per gli incaricati al trattamento la documentazione tecnica al fine di garantire la qualità e la correttezza dei dati durante la fase della raccolta e i successivi trattamenti. La maggior parte di tali misure sono disponibili su web.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;

L'Ente ha adottato il Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach (Determinazione n. 212807/2018) e la procedura per la gestione degli incidenti di sicurezza e data breach (con documento registrato nel protocollo regionale).

Tali documenti mirano alla corretta gestione degli incidenti di sicurezza che è misura che consente di evitare o di minimizzare la compromissione dei dati dell'organizzazione in caso di incidente.

Sono inoltre definite le modalità di registrazione e mantenimento dei log di audit relativi agli accessi e alle attività eseguite dagli utenti sui sistemi e agli eventi di sicurezza. In particolare, la piattaforma di Log Management in uso garantisce il mantenimento dei requisiti di riservatezza, integrità e disponibilità degli eventi di log.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);

Il Servizio ICT ha definito una procedura (Procedura di Restore) per il ripristino dei dati ed un Piano di Business continuity per garantire la continuità dei servizi IT a fronte di uno scenario di disastro. L'Ente verifica a intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse. Sono implementati meccanismi di ridondanza su tutte le strutture elaborative che contribuiscono a erogare servizi critici, secondo quanto rilevato attraverso la "Business Impact Analisys (BIA)".

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;

Al momento della dismissione i dati presenti sugli strumenti elettronici sono cancellati in maniera sicura o attraverso formattazione a basso livello, wiping, smagnetizzazione o distruzione fisica prima del loro riutilizzo e della loro dismissione, come indicato esplicitamente nella policy dedicata agli Amministratori.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Sono state applicate diverse misure tecniche per garantire la trasmissione sicura di tutti i dati che transitano nell'Ente, in particolare la trasmissione dei dati su canali cifrati (es. HTTPS, SFTP, SSH, Host-on-demand over SSL, ecc.); la protezione a mezzo del protocollo di crittografia TLS 1.1 e meccanismi di cifratura delle comunicazioni verso i Database Oracle.

Comune di Firenze

MISURE ORGANIZZATIVE

- Il Responsabile per la protezione dei dati (RPD) del Comune di Firenze, in base alla convenzione stipulata con la Città metropolitana, è il dott. Otello Cini. Ciascun Direttore/Dirigente è stato individuato come responsabile/sub-titolare dei trattamenti dei dati afferenti al proprio assetto organizzativo.
- Ogni Direttore/Dirigente del Comune di Firenze può pertanto nominare fra i propri collaboratori gli "Incaricati/autorizzati del trattamento".
- Il Comune di Firenze ha organizzato due giornate di corso per illustrare il regolamento UE ai dipendenti e successivamente è stato sottoposto un corso online.
- Vengono effettuati monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679 nonché vengono pianificati i controlli interni periodici.
- In caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per conto del Comune di Firenze, il Direttore/Dirigente nomina il responsabile esterno e redige un 'contratto' in cui si definiscono la materia, la durata, la finalità del trattamento, il tipo di dati personali, la categoria di interessati e gli obblighi del responsabile.
- per le sale server è attivo il controllo fisico degli accessi.
- Il Comune di Firenze ha predisposto diverse informative per il conferimento delle informazioni agli interessati ove è specificato l'indirizzo e-mail cui rivolgersi per l'esercizio dei diritti;
- in caso di contitolarità del trattamento, è prevista la sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679.
- il materiale cartaceo inerente la gestione del personale (in special modo quello contenente dati sensibili) deve essere conservato in luoghi chiusi a chiave (armadi, schedari, ecc.) evitando di lasciarlo sulle scrivanie o in luoghi non sicuri se non per il tempo strettamente necessario per la sua lavorazione e gli addetti alle segreterie del personale devono inoltre mantenere la massima riservatezza riguardo a tali dati e informazioni;

MISURE TECNICHE

- Il Comune di Firenze ha predisposto sistemi di autenticazione individuale degli utenti, sistemi di autorizzazione (profilazione applicativa) e sistemi di protezione (antimalware, antivirus, antiphishing, antispam; firewall; navigazione web protetta);
- Sono adottate misure per garantire la sicurezza delle postazioni fisiche di lavoro, con definizione di regole per la custodia e l'utilizzo sicuro delle dotazioni assegnate (dispositivi portatili, supporti rimovibili ecc.)
- Sono stati adottati sistemi perimetrali di controllo; sono previste tecniche di cifratura per particolari tipi di dati e la pseudonimizzazione quando i dati personali non sono più necessari per il trattamento specifico.
- Adozione di misure per garantire la qualità e la correttezza dei dati.
- È prevista l'immediata segnalazione alla Direzione Sistemi Informativi di eventi che possano minare la sicurezza dei sistemi o costituire violazione dei dati personali (rilevazione di virus, perdita di dati, accessi indebiti / diffusione di dati non autorizzata). nei casi di incidente fisico o tecnico (perdita o furto): per le sale server sono attive misure antincendio e continuità operativa in caso di mancanza di corrente tramite l'impiego di gruppi di continuità (UPS) e gruppi elettrogeni; inoltre è attivo un sistema centralizzato di backup e sistemi di copiatura e memorizzazione di alcuni archivi elettronici.
- È stata definita la procedura per la cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Vengono adottate modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Comune di Milano

MISURE ORGANIZZATIVE

Assetto organizzativo interno al Comune di Milano per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento, così come definito nella Disciplina del nuovo Modello organizzativo Privacy del Comune di Milano (Appendice n.9 al Regolamento sull'Ordinamento degli Uffici e dei Servizi) introdotta con Deliberazione di Giunta Comunale n.914 del 25/5/2018.

La citata Appendice n.9 al Regolamento sull'Ordinamento degli Uffici e dei Servizi del Comune di Milano nello specifico:

- all'art. 3.3.2. individua il Data Protection Officer - DPO, come previsto dall'art.16bis del Regolamento sull'Ordinamento degli Uffici e dei Servizi.
  Nell'ambito del vigente assetto organizzativo del Comune di Milano, l'Unità Privacy fornisce supporto al DPO in relazione alle funzioni allo stesso spettanti. Tale Unità è collocata nell'ambito della Direzione Generale, alle dirette dipendenze del Direttore Operativo.
  Fermo restando le funzioni descritte negli artt. Da 37 a 39 del GDPR, i compiti specifici affidati al DPO sono dettagliati nel relativo atto di nomina, ovvero in specifici atti successivi.
- all'art. 3.3.3. definisce funzioni e ruoli del personale dirigente.
  Al personale dirigente, in relazione e nei limiti delle competenze facenti capo alla posizione di responsabilità ricoperta, è rimesso il presidio in tema di protezione dei dati personali, anche attraverso l'esercizio dei compiti descritti nella declaratoria di dettaglio di cui all'art. 3.3.3.della citata Appendice n.9.

- Interventi per la formazione del personale, come da Programma formativo del Comune di Milano, che prevede una formazione specifica per tutto il personale dell'ente in base alle funzioni e ai ruoli.
- Adozione di un sistema informatico centralizzato per il monitoraggio e l'aggiornamento del Registro dei trattamenti del Comune di Milano ai sensi dell'art.30 del Regolamento (EU) 2016/679.

MISURE TECNICHE

L'art. 3.3.1 dell'Appendice n.9 al Regolamento sull'Ordinamento degli Uffici e dei Servizi demanda, in via esclusiva, alla Direzione Sistemi Informativi e Agenda Digitale le funzioni, le attività e le responsabilità connesse ai profili tecnico-informatici, con particolare riguardo alla gestione della sicurezza dei sistemi informativi, anche distribuiti, degli applicativi, delle reti di telecomunicazioni e della sicurezza fisica del Data Center.

CREA

MISURE ORGANIZZATIVE - Commercio con l'estero (CRE-00020)

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati): Il titolare del trattamento dei dati è Roberto Solazzo, referente per le attività relative all'analisi del commercio con l'estero presso il CREA PB, con sede in Roma, Via Po, 14.

Il Responsabile del trattamento dati è il Direttore del Centro di Politiche e bioeconomia del CREA (CREA-PB)

- Gestione delle autorizzazioni all'accesso ai dati: info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

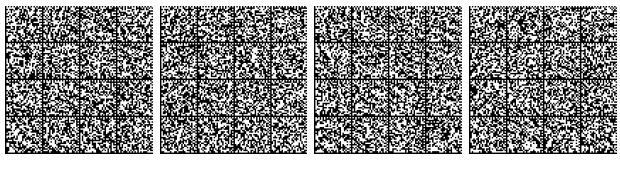
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati : Implementazione di un sistema informatico di verifica del rispetto delle regole di riservatezza delle elaborazioni territoriali riguardanti il commercio con l'estero (specificate nella sezione Misure tecniche), con l'oscuramento delle elaborazioni che non rispettano tali regole.

MISURE TECNICHE - Commercio con l'estero (CRE-00020)

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi: - info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro: tutte le postazioni individuali di lavoro sono dotate di computer con accesso personale gestito con il sistema Activity Directory di Microsoft

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati: Le elaborazioni territoriali svolte dal CREA sul commercio estero riguardano esclusivamente i flussi di interscambio commerciale e non gli operatori del commercio con l'estero. Pertanto alle stesse viene applicato il principio di riservatezza passiva e quello di riservatezza attiva, con l'oscuramento delle voci e delle elaborazioni che non rispettano tali vincoli. In particolare, per la riservatezza attiva viene applicata la regola dei tre operatori, condizionata alla verifica dell'assenza di posizione dominante da parte di una delle imprese (con una soglia di quota detenuta pari all'80% del totale al netto del secondo principale operatore).



Inoltre, a livello merceologico viene effettuata una riaggregazione delle oltre 2500 voci NC8 relative all'agroalimentare in 279 aggregati, secondo una classificazione sviluppata dal CREA-PB. Tali aggregati rappresentano il massimo livello di dettaglio merceologico di diffusione delle elaborazioni.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679: info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto): info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche: info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni: la trasmissione dei dati sia all'interno del CREA che all'esterno dell'Ente, avviene solo in modalità aggregata e nel rispetto delle norme di riservatezza sopra descritte.

MISURE ORGANIZZATIVE - Rete d'informazione contabile agricola (CRE-00001)

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati): - Il Titolare del trattamento dei dati personali è CREA - Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria, con sede legale in Roma, Via Po, 14. Il Responsabile del trattamento dati è il Direttore pro tempore del Centro di Politiche e bioeconomia del CREA (CREA-PB)

- Gestione delle autorizzazioni all'accesso ai dati: L'accesso ai dati individuali (https://bancadatirica.crea.gov.it/Default.aspx) è riservato ai soli utenti afferenti al Sistema statistico nazionale (SISTAN), attraverso credenziali personali rilasciate dal CREA-PB.

La pagina di accesso contiene le NOTE LEGALI, riportanti le indicazioni circa il Copyright e diritti d'autore, il Disclaimer (Esclusione di responsabilità) e la Privacy e segreto statistico.

- modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati"): consegna della cosiddetta "Lettera al conduttore" con la quale si informa il conduttore agricolo della finalità dell'indagine, del tipo di collaborazioni richiesta e si chiede formale adesione all'indagine con conseguente sua sottoscrizione. Nella stessa Lettera sono riportati i riferimenti normativi al Segreto statistico, all'Obbligo di risposta e alla Tutela della riservatezza e diritti degli interessati

- in caso di contitolarità del trattamento, sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679: Accordo di collaborazione con ISTAT per l'effettuazione in forma coordinata dell'indagine RICA e dell'indagine REA

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati: consegna della cosiddetta "Lettera al conduttore"

MISURE TECNICHE – Rete d'informazione contabile agricola (CRE-00001)

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi: utenti coordinatori nazionali e regionali indagine RICA: accesso al Server con gli archivi contabili nazionali distinti per Esercizio contabile con autenticazione attraverso nome utente e password definite secondo le regole di sicurezza e persistenza. Accessi monitorati attraverso funzioni specifiche definite all'interno dell'engine di MS SQLSERV. Database ad accesso riservato ai soli responsabili dell'indagine.

Utenti CREA e utenti SISTAN: accesso all'applicativo online BDR (https://bancadatirica.crea.gov.it) gestito dal coordinamento nazionale dell'indagine. Utenti accreditati con nome utente e password. Sistema di monitoraggio degli accessi e delle elaborazioni richieste al sistema.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro: - tutte le postazioni individuali di lavoro sono dotate di computer con accesso personale gestito con il sistema Activity Directory di Microsoft

- Adozione di misure per garantire la qualità e la correttezza dei dati: - il controllo qualitativo dei dati raccolti nell'ambito dell'indagine RICA è garantito dalle regole definite dalla metodologia e dalla messa in atto di un sistema di controllo di qualità sui singoli dati rilevati a livello di azienda agricola.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679: - info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto): info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche: - info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni: La trasmissione dei dati sia all'interno del CREA che all'esterno dell'Ente avviene secondo regole che consentono di garantire il segreto statistico. I microdati disponibili nella BDR Online non contengono alcuna informazione identificativa del rispondente all'indagine RICA. Le elaborazioni vengono trasmesse solo in modalità aggregata; inoltre nei casi con meno di 5 osservazioni il dato viene oscurato.

MISURE ORGANIZZATIVE - IV Studio sui Consumi Alimentari in Italia (IV SCAI) - programma EU-MENU (EFSA), popolazione 10-74 anni (CRE-00022)

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati): - Il Titolare del trattamento dei dati personali è CREA - Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria, con sede legale in Roma, Via Po, 14. Il Responsabile del trattamento dati è il Direttore del Centro di Ricerca Alimenti e Nutrizione (CREA-AN)

- Gestione delle autorizzazioni all'accesso ai dati: - L'accesso ai dati individuali è consentito ai soli rilevatori, i dati sono crittografati e saranno completamente anonimizzati alla fine del trattamento di base

- Interventi posti in essere per la formazione del personale: - I rilevatori reclutati per la raccolta dei dati sono stati istruiti

Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto: responsabile del trattamento dei dati inseriti nel sistema software Dev4U S.r.l.s. gestore del sistema

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati"): - I partecipanti o genitori/tutori ricevono l'informazione sulle finalità e le modalità dello studio, viene richiesto loro di firmare il modello di consenso informato.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati: - la lettera informativa contiene i riferimenti da contattare in caso di necessità

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei: - i dati riportati su

supporto cartaceo (questionari a corredo della raccolta dei dati alimentari) sono distaccati e conservati separatamente
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati : Per i minori è richiesto il consenso di un genitore o tutore e le interviste sono effettuate alla presenza di un adulto responsabile

MISURE TECNICHE - IV Studio sui Consumi Alimentari in Italia (IV SCAI) - programma EU-MENU (EFSA), popolazione 10-74 anni (CRE-00022)
- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi: i rilevatori sono dotati di credenziali personali
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro: tutte le postazioni individuali di lavoro sono dotate di computer con accesso personale gestito con il sistema Activity Directory di Microsoft
- Adozione di misure per garantire la qualità e la correttezza dei dati: il primo controllo dei dati viene effettuato nel corso di ciascuna intervista (computer assisted personal interview - CAPI), successivamente il MASTER che riceve tutti i dati effettua un controllo, reinviando le correzioni al rilevatore. Il processo si chiude quando non sono più evidenziati errori. Il secondo controllo viene effettuato massivamente su tutti i dati inseriti. Il terzo controllo avviene nella fase di trasferimento delle informazioni al sistema DCF dell'EFSA.
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679: info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto): info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche: info disponibili presso l'ufficio Sistemi Informativi dell'amministrazione centrale del CREA
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni: In sede di trasferimento dei dati una volta validati dal completamento dell'iter dei controlli, saranno resi disponibili completamente anonimizzati e i microdati resi disponibili ad un livello di aggregazione minimo (matrice dei dati) in modo da mettere in grado gli utenti di elaborare dati

Gestore dei Servizi Energetici (GSE)

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)
Il GSE si è dotato di un assetto organizzativo *compliant* al GDPR. In data 24 maggio 2018 è stato nominato dal Consiglio di Amministrazione il Responsabile per la protezione dei dati personali a cui fa capo un Ufficio di supporto, che opera in posizione di autonomia e terzietà e a diretto riporto del Vertice. Le figure apicali delle Strutture aziendali rivestono il ruolo di Soggetti Designati, ai quali sono ricondotte le responsabilità dei trattamenti di specifica competenza. I dipendenti sono stati autorizzati al trattamento dei dati personali cui hanno accesso per l'assolvimento dei propri compiti. La Direzione Legale svolge funzioni di supporto giuridico a tutti i soggetti di cui sopra.
- Gestione delle autorizzazioni all'accesso ai dati
La gestione delle autorizzazioni di accesso ai dati è oggetto di una specifica procedura aziendale che prevede tra l'altro l'identificazione e la nomina formale degli *owner* delle applicazioni aziendali, ossia dei soggetti responsabili (in genere le Figure apicali di cui sopra) dell'autorizzazione agli accessi e delle profilazioni applicative.
- Interventi posti in essere per la formazione del personale
L'Ufficio RPD ha già posto in essere tra la fine del 2018 ad oggi i primi corsi di formazione destinati sia ai soggetti che rivestono posizioni apicali che alla generalità della popolazione aziendale. Per i dipendenti che gestiscono dati di natura particolare e/o giudiziaria sono state previste anche specifiche giornate formative di natura tecnico specialistica oltre che giuridica.
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici
L'Ufficio RPD tra la fine del 2018 e i primi mesi del 2019 ha proceduto ad effettuare un vero e proprio assessment dei trattamenti aziendali e dei dati trattati, formalizzando una seconda versione aggiornata del Registro delle attività di trattamento all'agosto del 2019.
Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
Per il settore in cui opera il GSE (settore energetico) non risultano allo stato approvati Codici di Condotta né sussistono meccanismi di certificazione formalmente riconosciuti. Tuttavia, l'Ufficio RPD mantiene rapporti di confronto con i principali operatori del settore energetico e ha partecipato a convegni, corsi di formazione e eventi in materia di privacy e di cybersecurity. Il GSE, in occasione del conferimento di contratti affidati ai sensi del Codice dei contratti pubblici, provvede a designare le società fornitrici quali Responsabili Esterni del Trattamento ai sensi dell'art. 28 del GDPR e/o Amministratori di Sistema ogni qualvolta ad essi vengano affidati dati personali nell'ambito delle prestazioni contrattuali e/o la gestione di sistemi /applicativi contenenti dati di tal genere.
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi
Il controllo fisico degli accessi alle Server Farm è gestito mediante opportuni lettori di badge posti all'ingresso dei locali stessi, al fine di garantire l'accesso ai soli utenti autorizzati alla gestione e manutenzione degli impianti a supporto e dei sistemi IT. All'interno delle Server Farm sono presenti inoltre dei sensori per la gestione di eventuali situazioni di emergenza (incendi, allagamenti, ecc.).
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")
Il GSE informa i propri interessati sia attraverso la privacy policy di contenuto "generale" presente sul proprio sito istituzionale, sia attraverso le informative "dedicate" in occasione dell'accesso agli specifici trattamenti e della stipula di contratti.
- In caso di contitolarità del trattamento, sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679
Non sono ad oggi presenti in GSE accordi di contitolarità.
- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati
Il GSE garantisce ai soggetti interessati la possibilità di esercitare i diritti riconosciuti dal GDPR mediante gli appositi canali di comunicazione presenti sia sul sito istituzionale, sia nei portali dedicati alle attività di core business orientati ai beneficiari degli incentivi e delle forme di sostegno in tema di rinnovabili ed efficienza energetica.
Ulteriori richiami ai diritti esercitabili dagli interessati sono contenuti nelle convenzioni e negli atti contrattuali in cui è controparte il GSE, in qualità di Titolare del trattamento.
- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei

Il GSE è dotato di un proprio servizio di guardiania e di videosorveglianza che garantisce il controllo sugli accessi nei propri locali, nonché di archivi per la documentazione cartacea dotati di chiavi e con accesso controllato.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

In generale i dati personali trattati dal GSE nei processi di *core business* non ricadono nella categoria di dati particolari né la Società ha, di regola, rapporti con soggetti interessati "vulnerabili".

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

Il GSE, attraverso l'utilizzo di una piattaforma di Identity Access Management centralizzata, attua misure tecniche per la corretta identificazione e autenticazione degli utenti (siano essi interni o esterni). Viene così garantito l'accesso ai dati gestiti dai sistemi informatici aziendali per i soli utenti autorizzati. Le utenze utilizzate per l'accesso ai sistemi IT sono profilate sulla base delle specifiche esigenze aziendali. Le credenziali di accesso univoche rispettano inoltre specifici criteri di sicurezza in termini di complessità, lunghezza e durata. Sono definite delle policy di sicurezza, basate sugli specifici profili utente per l'accesso alle risorse aziendali specifiche. Il tracciamento degli accessi viene eseguito sia in modo diretto sulle piattaforme che erogano gli stessi servizi IT che utilizzando una piattaforma centralizzata di gestione dei Log in via di potenziamento.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Riguardo alla protezione delle postazioni fisiche di lavoro e all'utilizzo delle stesse da parte degli utenti, sono adottate dal GSE misure di sicurezza per il rilevamento e blocco dell'esecuzione di possibili software dannosi (quali malware, virus, …), misure per il controllo centralizzato del servizio di navigazione Internet, sistemi di aggiornamento del sistema operativo, e politiche di sicurezza associate al profilo utente per il controllo dell'accesso ai servizi informatici aziendali. Tali strumenti sono gestiti e mantenuti aggiornati in modo centralizzato e consentono l'implementazione di processi controllati per il deploy e l'upgrade costante delle postazioni fisiche di lavoro

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

L'infrastruttura di rete del GSE attraverso la quale sono erogati i servizi informatici aziendali prevede diversi livelli di segregazione che corrispondono ai differenti ambienti operativi, realizzati mediante l'utilizzo di piattaforme tecnologiche quali apparati di rete e sicurezza (Es. Firewall), che consentono l'applicazione delle politiche di controllo sui flussi traffico. Il GSE inoltre ha adottato soluzioni tecnologiche per la cifratura delle risorse di storage e delle postazioni di lavoro mobili (notebook e portatili), avviando una implementazione graduale di tale misura, al fine di aumentare la protezione delle informazioni aziendali. È in corso di completamento il progetto che prevede la cifratura dei principali database aziendali.

- Adozione di misure per garantire la qualità e la correttezza dei dati

Il GSE al fine di garantire la qualità nell'erogazione dei propri servizi IT a tutela e protezione del patrimonio informativo aziendale, ha implementato un processo di attuazione dei controlli previsti dalle Misure Minime di sicurezza ICT per le pubbliche amministrazioni emanate dall'AGID. Tale processo prevede tra gli altri il processo di nomina degli amministratori di sistema, un adeguato livello di profilatura per le utenze che possono accedere alle applicazioni di propria competenza.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

Il GSE adotta una procedura per la gestione degli incidenti informatici e implementa un servizio di monitoraggio degli eventi finalizzato alla rilevazione di eventuali anomalie e violazioni informatiche attraverso una struttura dedicata di tipo SOC (Security Operation Center). La raccolta degli eventi ai fini della sicurezza informatica prevede l'utilizzo di tecnologie centralizzate di tipo SIEM (Security Information Event Management) in corso di consolidamento sia tecnologico che funzionale al fine di aumentare il perimetro e l'efficacia del monitoraggio della sicurezza. Tali strumenti sono previsti a supporto anche del processo di analisi e identificazione dei potenziali Personal Data Breach. La gestione di questa ultima tipologia di eventi è regolamentata a livello aziendale da una specifica procedura, che descrive il processo di attuazione degli adempimenti previsti dal Regolamento UE 2016/679 per quanto previsto dalla funzione aziendale del RPD. Altre attività funzionali alla gestione degli eventi e al rilevamento delle anomalie di sicurezza, riguardano l'implementazione di misure tecniche per la difesa e la prevenzione da potenziali malware, per il controllo del traffico WEB e per la gestione della posta indesiderata (antispam). Nell'ambito della Threat Intelligence è in corso di sviluppo un progetto per l'implementazione di un sistema opensource per la raccolta ed aggregazione di Indicatori di Compromissione utili al potenziamento del monitoraggio e contrasto delle minacce cyber.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

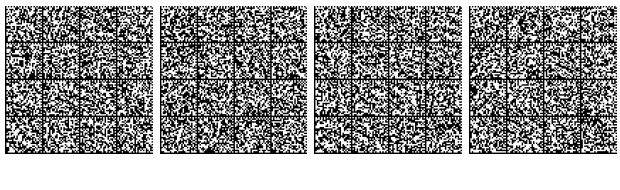
A tutela del patrimonio informativo aziendale è definito e implementato un processo di Backup che prevede una copia di sicurezza dei dati e delle configurazioni aziendali, attraverso l'utilizzo di tecnologie dedicate e distribuite su sistemi di storage locale, sistemi a nastro anche su siti esterni e la replica asincrona su un sito remoto utilizzato ai fini della continuità operativa. Le copie dei dati sono utilizzate in caso di perdita parziale o totale delle informazioni che sono soggette a backup. Sono inoltre previste soluzioni finalizzate a garantire il recupero dei dati, il ripristino delle applicazioni e dei sistemi ICT in un'ottica di continuità operativa per i servizi di business aziendali, sia in caso di perdita che in caso del verificarsi di incidenti tecnici. Il GSE dispone di un sito dedicato per il Disaster Recovery che viene inserito nella strategia di continuità operativa aziendale, finalizzato ad assicurare la possibilità di disporre di una piattaforma tecnologica da utilizzare in caso di disastro naturale o ambientale tale da rendere indisponibili i normali siti di erogazione dei servizi ICT. La disponibilità dei dati e dei servizi informatici viene garantita anche attraverso la distribuzione dei sistemi e delle infrastrutture ICT su due siti distinti in configurazione di alta affidabilità, dove è prevista la replica dei dati in modalità sincrona con il supporto di tecnologie per la virtualizzazione dei sistemi ICT.

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

Il GSE è dotato di un sistema per la cancellazione sicura e certificata delle informazioni registrate sui dispositivi di memorizzazione (hard-disk, dischi storage, memorie, dispositivi mobili) tali da consentire che i dati fisicamente presenti sugli stessi non possano essere recuperati applicando specifiche procedure tecniche. È prevista anche l'implementazione di un processo per la distruzione sicura dei supporti di memoria in caso di guasto irreversibile dei dispositivi.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

Al fine di garantire l'integrità, la disponibilità e la riservatezza delle informazioni, il GSE implementa meccanismi di cifratura per la protezione delle comunicazioni, dei servizi web esposti sul perimetro esterno e dei flussi informativi interni dove transitano dati personali o ritenuti strategici a livello aziendale. Tali servizi di sicurezza sono realizzati anche attraverso l'utilizzo dei certificati digitali, del protocollo TLS e di servizi HTTS. Il GSE dispone anche di una rete interna realizzata con tecnologia wireless che prevede l'implementazione delle misure di sicurezza in termini di controllo accessi, profilatura e cifratura del canale di comunicazione. Per la gestione delle connessioni di utenti esterni al perimetro aziendale laddove previste e dei collegamenti tra i siti remoti sono implementati differenti tipologie di connessioni sicure VPN attraverso le quali sono garantiti i requisiti di riservatezza e integrità dei dati in transito.



Inail

Piani di sicurezza
- Piano di sicurezza applicativa: Analisi dei rischi semplificata per le applicazioni; strumento adottato per il *byDesign
- Piano di sicurezza infrastrutturale: Analisi dei rischi semplificata per i progetti infrastrutturali; strumento adottato per il *byDesign
Autenticazione
- Access management e SSO (IAA): Soluzione standard
- Autenticazione su LDAP di dominio: Usato in alternativa a 'Access Management e SSO' solo per App intranet; non accettato LDAP esterno.
- Strong authentication: Implementata per un insieme ristretto di applicazioni
Autorizzazione
- Sistema di autorizzazione e profilazione: Soluzione standard
- Profilazione per configurazione AD (Gruppi): Alternativa a 'Sistema di autorizzazione e profilazione'. Non è permessa la profilazione applicativa.
Audit e monitoraggio
- Tracciatura applicativa: Soluzione standard
- Logging applicativo degli eventi di sicurezza: In subordine alla tracciatura applicativa
- Attività di audit dedicata: Implementata per un insieme ristretto di applicazioni
- Log management/SIEM (Archiviazione sicura dei log amministrativi): Soluzione standard
- Tracciatura esterna per scambio dati in convenzione: Per il tramite delle soluzioni cloud based utilizzate per lo scambio di file
Protezione dei dati
- Crittografia database: o alternative adeguate (es.: cifratura applicativa) se opportunamente motivate
- DLP e classificazione delle informazioni: In fase di adozione
- Database security gateway (DBAM): Soluzione standard
- Mascheramento dei dati in ambiente di collaudo: Soluzione standard
- Crittografia di rete e certificati SSL: Soluzione standard
- Minimizzazione/Aggregazione: Per scambio dati in convenzione
- Integrazione con il sistema di firma digitale: Per fini di integrità e non ripudio
Protezione del software
- Documentazione tecnica adeguata: Soluzione standard
- Test di sicurezza applicativa: Soluzione standard
- Scrittura di codice sicuro: Soluzione standard
- Vulnerability Assessment: Soluzione standard
- Patch management, hardening dei server: Soluzione standard
- Test in ambiente di certificazione: Soluzione standard
Disponibilità dati e servizi
- Soluzioni di HA: Soluzione standard
- Backup e Restore: Soluzione standard
- Soluzioni di DR (Piano di continuità dedicato): Per soluzioni critiche in termini di disponibilità
Sicurezza rete
- Reverse proxy: Soluzione standard
- IPS: Soluzione standard
- WAF: Soluzione standard
Cloud e API
- API gateway: Implementata per un insieme ristretto di applicazioni
- Soluzioni ad hoc per il cloud: Implementata per un insieme ristretto di applicazioni
Dati di minori
- Adeguata base legale per i trattamenti dei dati di minori: I trattamenti non si basano sul consenso
- Registrazione al portale controllata: È inibita la registrazione al portale istituzionale dei minori di anni 14
Formazione e awareness
- Formazione del personale: Soluzione standard

Termini ed Acronimi
DCOD: Direzione Centrale per l'Organizzazione Digitale; WAF: Web Application Firewall; DBAM: Database Activity Monitoring; DLP: Data Loss Prevention; LDAP: Lightweight Directory Access Protocol; SSO: Single Sign-On; IAA: Identification, Authentication and Authorization; SIEM: Security information and event management

Istituto Nazionale per l'Analisi delle Politiche Pubbliche (INAPP)

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento
Il Presidente Inapp è il titolare del trattamento dei dati prodotti dall'Istituto. Oltre agli uffici dirigenziali l'organigramma corrente dell'Inapp prevede la presenza di 4 strutture di ricerca, di 2 progetti strategici e di 4 servizi trasversali che fanno capo alla Direzione Generale (Servizio Statistico, Servizio per la Comunicazione e divulgazione scientifica; Servizio Sistemi informativi e automatizzati; Servizio Programmazione). Il trattamento dei dati personali connessi ai lavori statistici presenti sul PSN coinvolge in primis le strutture di ricerca, nelle quali sono incardinate attività che prevedono l'acquisizione e l'elaborazione di dati personali; il Servizio Statistico, che ha il compito di controllare, conservare e diffondere, sia internamente che all'esterno, le banche dati di titolarità dell'Istituto, ed infine il Servizio Sistemi Informativi e automatizzati (SIA), che gestisce le politiche di sicurezza dell'Istituto e conseguentemente anche dei dati. Per ciascun lavoro presente sul PSN è identificato un responsabile del lavoro statistico, riportato nelle schede PSN.

- Gestione delle autorizzazioni all'accesso ai dati

Le autorizzazioni per l'accesso ai dati sono gestite dal Servizio Statistico, che a seguito di formale richiesta tramite modulistica predefinita valuta la pertinenza della richiesta e provvede, in caso di esito positivo, alla trasmissione delle informazioni. Il modulo per la richiesta dati da parte di dipendenti INAPP è stato predisposto in collaborazione con il Responsabile Protezione Dati sulla falsariga delle "Linee guida per l'accesso ai fini scientifici ai dati elementari del Sistan" adottate dal Comstat con direttiva n.11 del 7/11/ 2018. Per i ricercatori/soggetti esterni che fanno richiesta di dati elementari a titolarità INAPP è stato altresì predisposto, rifacendosi al modello adottato da ISTAT, un modulo ulteriore, adattato alle peculiarità dell'Istituto e aggiornato alle più recenti normative in materia di trattamento dati. In merito si fa presente che, alla luce dell'aggiornamento della modulistica relativa alle richieste di file di microdati per gli Enti SISTAN, in linea con la più recente normativa in materia di trattamento dei dati personali, si è valutata l'opportunità di rivedere nel breve termine i moduli INAPP di rilascio dati (ad interni e ad esterni) attualmente in uso dal Servizio Statistico.

- Interventi per la formazione del personale

Responsabile del Servizio Statistico e Responsabile Protezione Dati partecipano agli incontri formativi/informativi organizzati dall'Autorità privacy o dal SISTAN. Per i dipendenti delle strutture di ricerca e degli uffici amministrativi il Piano di Formazione 2019 ha previsto un corso di 3 giornate finalizzato a fornire conoscenze in materia di trattamento e protezione dei dati. È in corso una procedura negoziata (Determina n. 409/2019) per selezionare il fornitore del servizio, da individuarsi tra primarie organizzazioni specializzate nella formazione su materie giuridiche ed economiche.

- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto

Il conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno viene realizzato tramite apposito "accordo scritto", redatto secondo uno standard predisposto dal Responsabile per la Protezione dei dati personali, che viene sottoscritto dal legale rappresentante della società/ente esterno. Per quanto in particolare concerne attività di ricerca inserite nel PSN che implicano affidamenti con contratto a società esterne, l'Istituto, Titolare del trattamento e rappresentato legalmente pro tempore dal Presidente, procede con nota autorizzatoria a nominare il legale rappresentante della società o dell'RTI affidatario Responsabile del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679, integrando tale nota con ulteriori atti formali ad assicurare la conformità delle attività con la più recente normativa europea e nazionale in materia di trattamento dati, di segreto statistico e di tutela della riservatezza in generale.

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

L'informazione agli interessati nei trattamenti di dati personali connessi ai lavori statistici inseriti nel PSN è data attraverso la lettera che viene inviata a tutti coloro che sono coinvolti nelle indagini dirette o tramite apposita brochure allegata alla lettera. Tale lettera, di norma a firma del Presidente Inapp, è usualmente inviata agli interessati alcune settimane prima dell'avvio della fase di campo.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

Le indagini dirette che coinvolgono soggetti minorenni o la raccolta di dati sensibili condotte da Inapp sono volontarie e non prevedono alcun obbligo di risposta. Nel caso in cui un'indagine preveda il coinvolgimento di minorenni è prevista, inoltre, l'autorizzazione preventiva da parte del genitore o del tutore legale.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

Ogni unità di personale INAPP che utilizza strumentazioni informatiche si autentica come utente di dominio *active directory* sulla propria postazione di lavoro: senza tale livello di autenticazione l'utilizzo delle postazioni non è possibile. In aggiunta, il personale del Servizio SIA per poter accedere ai *repository* e ai sistemi di elaborazione che ha dedicato agli archivi statistici sui quali opera (per le ordinarie operazioni di stoccaggio pre-processamento e normalizzazione) utilizza un ulteriore livello di autenticazione e di comunicazione tramite il protocollo ssh/sftp configurato per accedere esclusivamente con scambio chiavi (pubblica e privata) . Tutte le chiavi di autenticazione sono salvate su files ystem criptato; l'autenticazione è possibile solo dalle postazioni di lavoro autorizzate (controllo IP tramite *firewall* dedicato) .

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/ o pseudonimizzazione

Le misure elencate di seguito sono inerenti alle attività svolte dal SIA in relazione alle banche dati statistiche per le quali è richiesto l'intervento del personal e specializzato tanto per l'acquisizione da soggetti esterni e relativo stoccaggio dei dati con criteri di sicurezza adeguati al trattamento dei dati personali, quanto per operazioni di normalizzazione, pre-processamento o linking dei dati raw. Le operazioni di stoccaggio dei dati vengono eseguite su server virtuali ospitati in cloud su datacenter e provider rispondenti alle attuali normative in vigore. I sistemi in cui risiedono i database sono protetti da un ulteriore firewall dedicato, che consente l'accesso esclusivamente dalle postazioni del personale SIA autorizzate. Tutti gli accessi e le attività sono sottoposte a un sistema di *logging*. È in fase di sperimentazione un meccanismo di rilevazione attiva. Database, estrazioni ed archivi vengono storati su f*ilesystem* criptati di tipo 'LuksEncription'.

- Adozione di misure per garantire la qualità e la correttezza dei dati

La qualità e la correttezza dei dati viene verificata dalle strutture di ricerca e dal Servizio Statistico tramite procedure predefinite. Il Servizio Statistico ha predisposto una Nota tecnica di supporto a tale attività ("Procedura per la validazione, l'archiviazione e la diffusione delle Banche Dati dell' INAPP"), nella quale sono dettagliate le procedure da adottare in fase di verifica della qualità delle banche dati ed in particolare nelle sub-fasi di verifica dell'esaustività e integrità della banca dati, della coerenza fra banca dati e documentazione allegata, della coerenza interna alla banca dati. Nella nota sono anche evidenziate le procedure da seguire nella fase di 'correzione dei dati'.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali {data breach} ai sensi dell'artico/o 33 del Regolamento (UE) 2016/679

Le risorse Cloud sono soggette a firewall attivi, perimetrali e IDS che rilevano e segnalano anche i tentativi falliti multipli, le attività di rete anomale o troppo invasive (es: scansioni insistenti, tentativi di *enumeration)* e bloccano con nuove regole e contromisure gli IP sorgenti. È in fase di sperimentazione un sistema di *intrusion detection* interno basato su OSSEC. Inoltre è stato previsto a bilancio 2020 il budget per presidi e strumenti specifici per incrementare il controllo accessi (videosorveglianza, controllo biometrico); la consulenza specifica per eseguire un audit di sicurezza atto ad integrare e potenziare le attuali misure; l'implementazione di un sistema di controllo delle connessioni remote con *logging* centralizzato e registrazione remota delle sessioni di lavoro, incluse quelle in *remotedesktop.*

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita of urto):

Backup delocalizzati, replica delocalizzata del nodo cloud.

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

È prevista la distruzione fisica dei dischi e dei supporti tramite apertura degli involucri protetti e azione deformante dei dischi magnetici o supporti. Tale operazione deve essere effettuata ogni volta che viene segnalata la dismissione o la sostituzione di supporti o hard drive delle apparecchiature hardware non escluse quelle su cui si sono operate estrazioni, query, elaborazioni tramite i consueti applicativi statistici (SAS, R, etc).

- Adozione di modalità di trasmissione dei dati a/l'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle

informazioni
La trasmissione di dati a società/ enti esterni viene effettuata sempre tramite canale FTP. I trasferimenti vengono effettuati tramite protocollo SFT over SSH con chiave a 4096 bit: le chiavi vengono scambiate tramite procedure concordate di volta in volta, che non prevedono la trasmissione in chiaro o la copia su supporti non sicuri. La trasmissione delle banche dati anonimizzate (nel formato di file standard), internamente o esternamente, viene effettuata sempre proteggendo le banche dati con password.

Invalsi

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati
All'interno di INVALSI le figure coinvolte nei trattamenti sono individuate sulla base dell'area organizzativa di appartenenza e del ruolo svolto.
In conformità all'art. 30 del GDPR è stato predisposto il Registro dei Trattamenti nel quale vengono specificamente individuati tutti i tipi di trattamento effettuati per i singoli ambiti di attività dell'INVALSI, con specifico riferimento alle macro-aree e ai vari progetti di ricerca condotti dall'Ente. Tale registro è predisposto, per competenza, da ciascuna area organizzativa con tutte le informazioni richieste dal Regolamento e aggiornato periodicamente sulla base dei cambiamenti normativi, organizzativi e tecnologici.
Nello specifico, all'interno del Registro dei Trattamenti, sono indicate, tra le altre, le seguenti informazioni:
- le aree organizzative Delegate al trattamento;
- il Referente dell'Unità organizzativa delegata al trattamento;
- le strutture che concorrono al trattamento;
- i soggetti esterni coinvolti nel trattamento;
- i soggetti esterni nominati Responsabili del trattamento, le persone autorizzate, gli amministratori di sistema.

In conformità alle disposizioni in materia di trattamento dei dati personali, è stato inoltre designato il Responsabile della protezione dei dati personali, soggetto esterno rispetto all'organigramma aziendale che svolge le attività ad esso attribuite dall'art. 39 del Regolamento europeo n. 2016/679 con le garanzie di indipendenza e di autonomia previste dalle disposizioni normative vigenti.
- Gestione delle autorizzazioni all'accesso ai dati
Ogni Responsabile di Area individua – nell'ambito della propria sfera di competenza – le persone autorizzate al trattamento dei dati, nonché i responsabili del trattamento di cui all'articolo 28 del citato Regolamento. La designazione di soggetti autorizzati nell'ambito del proprio assetto organizzativo avviene in forma scritta mediante la pubblicazione di una *Nomina a persona autorizzata al trattamento dei dati personali*, con definizione dell'ambito di autorizzazione al trattamento dei dati stessi.
L'accesso ai sistemi informatici, e ai relativi dati personali ivi contenuti, viene configurato dall'area dei sistemi informativi sulla base del ruolo del personale autorizzato e delle indicazioni del Responsabile dell'Area di competenza.
In caso di cambio mansione o termine del rapporto di lavoro da parte di una persona autorizzata, ogni Responsabile di Area, per competenza, fornisce opportuna e immediata comunicazione all'area dei Sistemi informativi per conseguente cambio o revoca delle autorizzazioni.
Pianificazione di controlli interni periodici
In coerenza con il Principio di Privacy by Design, il Responsabile della protezione dei dati personali viene coinvolto in occasione di nuovi progetti o interventi che possano avere un impatto sul trattamento dei dati personali, al fine assicurare un monitoraggio continuo del rispetto della normativa.
Con cadenza periodica, generalmente mensile, viene effettuato un incontro on site tra il Responsabile della protezione dei dati e i referenti INVALSI per allineamento sulle tematiche privacy e progetti che prevedono il trattamento dei dati personali.
È pianificata un'attività di verifica su base annuale al fine di valutare il livello delle misure tecniche e organizzative e definire le azioni di miglioramento necessarie. A seguito della verifica, il Responsabile della protezione dei dati, redige una relazione o una nota nella quale descrive il livello di rispondenza dei controlli alla normativa, le raccomandazioni per colmare gli eventuali gap riscontrati e le azioni di miglioramento.
- Adesione a codici di condotta e a meccanismi di certificazione
L'art. 2-quater del Codice Privacy fa salvi i codici di condotta vigenti per i trattamenti dati ai fini statistici, cui INVALSI ha aderito.
Inoltre, al fine di assicurare la tutela dei dati personali e diffondere la cultura della privacy a ciascuna persona autorizzata:
- viene consegnato il Regolamento interno con le istruzioni per il corretto trattamento dei dati personali;
- è erogata una sessione di formazione, che prevede in linea di massima i seguenti argomenti:
    - normativa di riferimento
    - modello organizzativo, ruoli e responsabilità
    - sistema sanzionatorio
    - rischi che incombono sui dati e misure di sicurezza
    - istruzioni per il corretto trattamento dei dati personali
    - casistiche particolari nell'ambito dei trattamenti svolti da INVALSI.

- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
In caso di trattamento dei dati svolto da soggetti esterni per conto dell'INVALSI, attraverso atti formali di designazione viene nominato un responsabile del trattamento ai sensi dell'articolo 28 del Regolamento europeo. La designazione di tali figure e l'individuazione delle relative funzioni viene formalizzata all'interno di appositi atti (sottoscritti dai Responsabili competenti per materia). I soggetti esterni designati quali *Responsabili del trattamento* sono tenuti al rispetto delle disposizioni e delle istruzioni fornite da INVALSI.
In particolare, in occasione di nuovi contratti che prevedono trattamenti di dati personali effettuati da soggetti esterni, l'Area acquisti predispone la bozza di nomina all'Area organizzativa richiedente per compilazione dell'ambito e modalità del trattamento. La lettera di nomina, ove necessario, viene sottoposta al DPO per verifica finale, quindi inviata al Responsabile del trattamento esterno per conseguente sottoscrizione. L'elenco dei Responsabili del trattamento deve essere conseguente integrato.
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi
L'accesso fisico all'Istituto è regolato attraverso l'utilizzo di badge personali con foto per tutti i dipendenti, un sistema di videocamere a circuito chiuso e una guardiania presidiata. Per i visitatori e i consulenti esterni è previsto l'accesso previa consegna di un documento di

riconoscimento e contatto con l'ufficio cui è diretto il visitatore. Ogni visitatore esterno è intestato al nominativo di un dipendente dell'Istituto che ne giustifica la necessità e firma il foglio della sua presenza. All'uscita, il visitatore consegna il foglio presenza sottoscritto dal referente INVALSI.

L'accesso alle aree riservate e alla cd. "Sala CED" è autorizzato al solo personale formalmente incaricato in base al principio di necessità.

- Modalità di conferimento delle informazioni ai sensi degli articoli 13 e 14 del Regolamento (UE) n.2016/679 ("informazioni agli interessati")

Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte dell'Istituto.

In caso di indagini dirette, che prevedono l'acquisizione dei dati direttamente presso gli interessati, viene loro preventivamente mostrato un link a una lettera informativa del Titolare del Trattamento. Nella lettera informativa sono descritte tutte le informazioni necessarie ai sensi dell'art. 13 del Regolamento UE 2016/679, in particolare le finalità del trattamento, le modalità in cui questo avviene, la possibilità che i dati rilevati possano essere utilizzati anche per ulteriori trattamenti statistici, nonché l'obbligatorietà o meno del conferimento dei dati. Contestualmente alla presentazione del link alla lettera informativa viene chiesto ai diretti interessati, ove applicabile, di esprimere un esplicito consenso attraverso una azione (come ad esempio la spunta di una casella) con la quale esprimono il proprio consenso al trattamento dei dati personali che li riguardano. Al termine della raccolta dei dati, il link al documento contenente la lettera informativa del Titolare del Trattamento, viene inviato anche via e-mail. Nei casi in cui i dati siano rilevati presso soggetti terzi e non sia agevole contattare gli interessati, l'informativa a questi ultimi viene resa attraverso il Programma Statistico Nazionale (PSN), l'atto di programmazione della statistica pubblica in cui sono descritte le caratteristiche di ciascun trattamento effettuato nell'ambito dei lavori statistici in esso inclusi.

In caso di casistiche particolari, la modalità di consegna e messa a disposizione dell'interessato dell'Informativa viene condiviso con il DPO.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

L'INVALSI garantisce l'esercizio dei diritti degli interessati come previsto agli articoli 15 e ss. del Regolamento europeo e in conformità alle disposizioni dell'articolo 89 del medesimo Regolamento, dell'art. 6-bis, comma 8, del decreto legislativo n. 322/1989 e dell'art. 11 delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale*. Ciascun interessato può esercitare i propri diritti attraverso le modalità indicate nell'Informativa. Il Referente dell'Area Organizzativa e trattamento di riferimento e il DPO, analizzano le richieste e condividono le risposte nei termini previsti dalla normativa. In caso di richieste particolari, o reiterate, coinvolgono il Rappresentante legale per condivisione delle decisioni in merito.

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei

L'INVALSI effettua prevalentemente trattamenti di dati personali su sistemi informatici. I trattamenti di dati cartacei, opportunamente indicati nel Registro dei trattamenti, sono effettuati in ossequio alle istruzioni consegnate alle persone autorizzate. In particolare, gli archivi cartacei vengono conservati presso i locali delle sedi di INVALSI opportunamente presidiati; al di fuori degli orari di lavoro o in caso di assenza del personale, i documenti cartacei sono conservati all'interno di armadi o uffici chiusi a chiave.

È inoltre vigente la "clean desk policy" al fine di non lasciare materiale cartaceo contenente dati personali incustodito e accessibile a persone non autorizzate.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

In presenza di categorie vulnerabili di interessati, viene effettuata una valutazione specifica sull'adozione di misure di sicurezza organizzative e tecniche adeguate al rischio per le libertà fondamentali degli stessi interessati.

In particolare, da un punto di vista organizzativo, ogni nuovo progetto/intervento che preveda categorie vulnerabili e/o dati particolari, viene discusso con il coinvolgimento del Responsabile della protezione dei dati al fine di comprendere le finalità e modalità di trattamento e le eventuali misure integrative da adottare.

In particolare, viene valutata la necessità di predisporre un Regolamento o procedura specifici per il progetto, oltre alla predisposizione delle Informative e l'individuazione dei soggetti autorizzati e dei Responsabili del trattamento.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

L'accesso alle infrastrutture tecnologiche dell'Istituto prevede l'utilizzo di credenziali di autenticazione individuali fornite ad ogni dipendente al momento dell'assunzione, con rinnovo obbligatorio ogni sei mesi. Le medesime credenziali (Single Sign-On) sono utilizzate dagli utenti abilitati per l'accesso dall'esterno alla rete informatica dell'Istituto tramite VPN di tipo SSL realizzata con i firewall.

L'accesso alle risorse informatiche offerte dai partner informatici dell'Istituto quali VPN, servizi di scambio file, applicazioni o database, necessita dell'utilizzo di credenziali di autenticazione individuali fornite ad ogni dipendente o collaboratore al momento della assegnazione di un ruolo o un compito all'interno del processo di lavoro. Le credenziali vengono obbligatoriamente rinnovate a cadenza regolare. Ogni accesso è tracciato e conservato per un periodo minimo di tre mesi.

L'autenticazione si basa sul principio che ogni utente che accede alle risorse del sistema deve essere univocamente identificato attraverso un codice, unico nel sistema e associato strettamente ad una persona fisica, che ne è responsabile dell'uso. La specifica risorsa informatica verifica le credenziali dell'utente e concede o meno l'accesso, tracciandolo nel sistema. L'utente può così accedere alla risorsa in base ai suoi profili di abilitazione.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

La sicurezza delle postazioni fisiche di lavoro (PC) è realizzata tramite:

- accesso attraverso le credenziali di autenticazione personali;

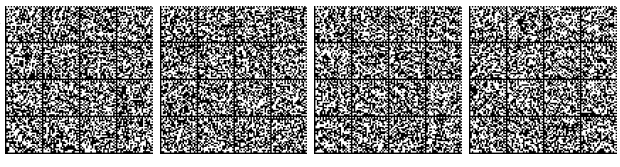
impostazione dello screensaver per evitare l'accesso da parte di personale non autorizzato in caso di spostamento dalla stazione di lavoro;

- accesso controllato all'edificio (servizio di portineria centralizzato);
- accesso controllato alle stanze (dotate di serratura).

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

- L'Istituto è dotato di un sistema di sicurezza perimetrale realizzato tramite firewall in configurazione HA (alta affidabilità). I firewall analizzano le richieste di accesso da/per la rete esterna ed effettuano controlli di sicurezza sul traffico della rete. Per fornire servizi all'esterno, senza compromettere la sicurezza della rete interna, sono state definite e implementate diverse zone logiche utilizzate da specifiche applicazioni. I firewall effettuano inoltre un controllo del traffico di rete per la rilevazione di anomalie e tentativi di intrusione.

- I dati personali provenienti da fonti amministrative, da rilevazioni statistiche o tramite l'acquisizione diretta dagli interessati, vengono sottoposti dall'Istituto a procedure di pseudonimizzazione nella fase immediatamente successiva la loro acquisizione e – in ogni caso – prima di ogni forma di utilizzo a fini statistici, inclusa l'integrazione con altre informazioni presenti nei registri statistici o altre fonti di dati. Le procedure di pseudonimizzazione prevedono dapprima la separazione dei codici identificativi diretti degli interessati dalle altre informazioni personali o di contesto. Tali codici identificativi vengono successivamente trasformati in pseudonimi e solo questi ultimi sono riattribuiti



alle altre informazioni personali o di contesto, al fine di consentire di effettuare in modo coerente le necessarie operazioni di elaborazione statistica tra fonti diverse o tra una stessa fonte nel tempo.
- La tabella di raccordo tra gli identificativi diretti e i codici pseudonimizzati è conservata separatamente su supporti crittografati ed utilizzata solo al fine di aggiornare il raccordo tra questi.
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati
In merito a progetti/interventi che prevedano la presenza di categorie vulnerabili di interessati o trattamento di particolari categorie di dati, viene effettuata una valutazione specifica sull'adozione di misure di sicurezza organizzative e tecniche adeguate al rischio per le libertà fondamentali degli stessi interessati.
Da un punto di vista delle misure di sicurezza tecniche, INVALSI adotta le seguenti misure valide per i dati personali particolari:
- la conservazione dei dati è realizzata separando i dati stessi su database relazionali differenti e indipendenti con una chiave univoca che rende possibile il collegamento dei dati tra loro;
- i database sono crittografati con diverse chiavi di cifratura simmetriche. Anche le connessioni ai database sono crittografate ed è utilizzato un certificato SSL (Secure Sockets Layer) per crittografare i dati trasmessi tra i database e le applicazioni client che si connettono agli stessi; la trasmissione dei dati INVALSI - MIUR avviene tramite FTP (File Transfer Protocol) protetto con HTTPS (HyperText Transfer Protocol over SecureSocketLayer) e proteggendo il contenuto dei file scambiati tramite crittografia asimmetrica;
- inoltre, lo scambio avviene solamente da indirizzi IP (Internet Protocoladdress) espressamente autorizzati; in merito poi all'accesso ai servizi di consultazione online questa avviene attraverso un applicativo predisposto da INVALSI nel rispetto del Provvedimento n. 393 del 2 luglio 2015;
- i servizi di consultazione online sono costituiti da moduli web sviluppati all'interno di un framework applicativo realizzato dall'INVALSI seguendo le linee guida descritte nella "PHP Security Guide" (http://phpsec.org/projects/guide/) a cura del PHP Security Consortium;
- l'accesso ai servizi di consultazione online previsti all'art. 4 e all'art. 6 del Regolamento sono fruibili attraverso la rete pubblica internet e sono protetti dal protocollo per la comunicazione sicura HTTPS (Hyper Text Transfer Protocol over SecureSocketLayer);
- l'accesso ai servizi online è consentito ai soli Dirigenti scolastici aventi classi di grado 8 (e nel 2019 anche di grado 13) nel proprio istituto, e solo se espressamente autorizzati dall'INVALSI;
- ai Dirigenti scolastici sono attribuite credenziali di accesso individuali il cui uso deve essere strettamente personale e non cedibile a terzi;
- le credenziali sono un codice per ogni Dirigente scolastico e una Password, composta in maniera tale da soddisfare adeguati requisiti di complessità e robustezza, da lui scelta
- l'accesso ai servizi di consultazione online sarà attivo esclusivamente nei periodi di interesse per le attività descritte nel Regolamento;
- l'accesso ai servizi di consultazione online è tracciato al fine di potere, in caso di necessità, risalire all'autore dell'accesso. Inoltre, al fine di prevenire e/o mitigare il rischio di accessi fraudolenti, l'INVALSI si riserva la facoltà di limitare l'accesso ai servizi di consultazione online solo in particolari fasce orarie;
- è in fase di predisposizione un sistema di cifratura dei dati.
- Adozione di misure per garantire la qualità e la correttezza dei dati
Un elevato livello di qualità delle statistiche ufficiali è da molti anni uno degli obiettivi che l'Istituto persegue regolarmente. La raccolta, la sincronizzazione, la conservazione e l'elaborazione dei dati avvengono attraverso un sistema integrato composto da:
- flussi informativi concordati con partner informatici e istituzionali;
- software specificamente sviluppato secondo elevati standard di sicurezza informatica;
- database relazionali i quali offrono strumenti propri quali chiavi primarie, chiavi esterne, relazioni e indici per la corretta gestione dei dati.
Il sistema descritto garantisce la qualità dei dati come definita dallo standard ISO/IEC 25012 "Data quality model" del 2008, nell'ambito dell'ISO, International Organization for Standardization.
Nel dettaglio, vengono garantite:
a) le caratteristiche inerenti al dato:
- accuratezza, intesa come perfetta rispondenza con il mondo reale che rappresenta;
- attualità, cioè del giusto tempo in cui il dato è utilizzato;
- coerenza, quindi un dato non contraddittorio con altri dati;
- completezza, presente per tutti gli attributi necessari;
- credibilità, proveniente da fonte certa.
b) le caratteristiche inerenti e dipendenti dal sistema:
- accessibilità: il dato è accessibile a tutti, anche dai disabili;
- comprensibilità: il significato del dato è chiaro, immediato o altrimenti documentato;
- conformità: il dato risponde a regolamentazioni specifiche;
- efficienza: il dato è utilizzabile con risorse accettabili e tempi adeguati allo scopo;
- precisione: il dato è del livello di misura necessario;
- riservatezza: il dato può essere utilizzato solo da utenti autorizzati;
- tracciabilità: gli accessi al dato sono registrati;
c) le caratteristiche dipendenti dal sistema:
- disponibilità: il dato necessario è disponibile e sempre interrogabile;
- portabilità: il dato può migrare da un ambiente all'altro con semplici procedure;
- ricoverabilità: il dato è salvato in un ambiente sicuro ed è recuperabile in caso di guasto delle apparecchiature.
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679
Le anomalie e gli incidenti aventi ripercussioni sul sistema informatico e sui livelli di sicurezza sono riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione al fine di minimizzarne l'impatto. L'individuazione di incidenti informatici in atto o avvenuti è resa possibile sia attraverso un apposito sistema di rilevazione degli attacchi installato nei punti critici della rete, sia attraverso l'accertamento di specifici eventi indicativi la cui rilevazione è affidata agli strumenti di monitoraggio.
All'atto della constatazione di un incidente, in corso o avvenuto, ne viene data immediata comunicazione al personale tecnico informatico che provvede ad analizzare la gravità della situazione e a riportarla al dirigente del servizio e alla Direzione generale.
I Servizi informatici hanno la facoltà di bloccare l'accesso alle specifiche risorse implicate se viene rilevato che queste stiano rappresentando una minaccia effettiva o potenziale per la sicurezza del sistema o per il suo corretto funzionamento (intrusioni dall'esterno, diffusione di virus, invio massivo di spam, furto delle credenziali di accesso).

L'intervento può riguardare il blocco immediato e momentaneo di un'utenza di posta, di un PC, di una applicazione, di una banca dati, di un server e, se necessario, del collegamento da remoto alla risorsa; in una fase successiva, il detentore della risorsa viene messo al corrente dell'accaduto e delle specifiche del caso.
L'Istituto ha inoltre stipulato con il CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche del Ministero dell'interno, Dipartimento della Pubblica Sicurezza Servizio di Polizia postale e delle comunicazioni un protocollo di intesa volto alla condivisione e all'analisi di informazioni idonee a prevenire e contrastare eventuali tentativi di diffusione abusiva dei quesiti; alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione; alla realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di crisi.
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)
L'Istituto effettua, con specifiche policy (frequenza e tipo di backup in relazione al grado di criticità e variabilità dei dati), i backup dei server, delle basi dati e dei repository condivisi e in uso alle diverse unità organizzative. Le intelligenze dei sistemi di memorazione utilizzati quali Storage Area Network (SAN) sono ridondate e le stesse consento di implementare meccanismi di protezione del dato da eventuali guasti (RAID).
È in fase di predisposizione un piano di continuità operativa che permette all'Istituto di affrontare in modo organizzato ed efficiente le conseguenze di eventi imprevisti garantendo il ripristino dei servizi critici in tempi e con modalità che consentano di ridurne le conseguenze negative.
L'Istituto ha sottoscritto con i propri partner informatici che offrono servizi di tipo infrastrutturale(IAAS) dei livelli di servizio (SLA) per la configurazione in modalità ridondata dei sistemi di memorizzazione critici con meccanismi di recupero delle informazioni dei sistemi server dell'ambiente distribuito e piani di backup sia dei server che dei database. I server si configurano come macchine virtuali in configurazione autonoma e indipendente con alta disponibilità realizzata mediante riavvio della macchina virtuale su diverso host in caso di guasto hardware dell'host sottostante al fine di garantire il ripristino e la disponibilità dei dati.
È stato predisposto un piano di continuità operativa che permette all'Istituto di affrontare in modo organizzato ed efficiente le conseguenze di eventi imprevisti garantendo il ripristino dei servizi critici in tempi e con modalità che consentano di ridurne le conseguenze negative.
I piani di manutenzione dei server prevedono backup giornaliero con conservazione dei backup per 30 giorni.
I piani di manutenzione dei database prevedono backup giornaliero con conservazione dei backup per 15 giorni.
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche
In attuazione alla normativa vigente, al fine di riutilizzare, dismettere o rottamare apparecchiature elettroniche su cui siano stati memorizzati dati personali, il personale competente provvede alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino e, ove tale cancellazione non fosse realizzabile, alla distruzione del supporto. La cancellazione sicura delle informazioni è effettuata tramite la formattazione dei dispositivi. Anche in caso di riutilizzo o dismissione di pc e server su cui siano stati memorizzati dati personali, è obbligatorio provvedere alla loro preventiva cancellazione sicura in maniera da renderne inintelligibile il contenuto.
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni
Lo scambio di dati con l'esterno avviene esclusivamente attraverso canali di comunicazione cifrati, nella fattispecie HTTPS oppure FTPS su canali cifrati (a seconda dei casi utilizzando SSL/TLS o una VPN), nella fattispecie:
- l'acquisizione dei dati attraverso applicazioni web (siti, web services) avviene tramite HyperText Transfer Protocol over SecureSocketLayer (HTTPS);
- lo scambio di dati tra partner informatici o istituzionali tramite SSH File Transfer Protocol (SFTP) e, a seconda del livello di servizio accordato, scambio attraverso crittografia asimmetrica a chiave pubblica/privata o rete privata virtuale (VPN);
- la trasmissione di dati all'interno avviene esclusivamente attraverso rete privata previo accesso con utenza e password personali.
- Archiviazione e conservazione dei dati
I dati personali o individuali trattati dall'Istituto con l'ausilio di strumenti elettronici sono archiviati e conservati in file o banche dati che risiedono su server gestiti a livello centrale. Non possono essere memorizzati su aree condivise pubbliche. I server appartengono:
- alla rete privata dell'Istituto;
- alle reti private dei partner informatici che offrono servizi di tipo infrastrutturale (IAAS) secondo livelli di servizio (SLA) concordati.
I dati personali o individuali non possono, pertanto, risiedere su singoli PC né possono essere memorizzati o duplicati su aree condivise pubbliche.
- Diffusione e comunicazione dei dati
È consentita la diffusione dei soli dati sui quali siano stati effettuati i necessari controlli per garantirne la rispondenza alle norme sul segreto statistico e sulla riservatezza. In ogni caso, i dati statistici prodotti possono essere diffusi solo in forma aggregata, in modo da non poter risalire all'identificazione degli interessati. Nei casi di diffusione di variabili in forma disaggregata, l'informazione sulle finalità e sulle modalità è fornita agli interessati mediante Informativa e sentito il parere dell'Autorità Garante per la protezione dei dati personali.
I Servizi informatici, previa autorizzazione della Direzione Generale, pubblicano dati – inerenti procedure di evidenza pubblica - sul sito web istituzionale (es. sezione sito web "Amministrazione trasparente").
L'ambito di comunicazione e diffusione per i singoli trattamenti sono descritti all'interno del Registro dei trattamenti e resi espliciti agli interessati attraverso l'Informativa.

Istituto nazionale della previdenza sociale - INPS

MISURE ORGANIZZATIVE
- La circolare n. 123 del 2015, attualizzata al Regolamento UE 2016/679, delinea l'assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e definisce i ruoli e le responsabilità dei soggetti coinvolti nel trattamento. È in corso di preparazione la nuova circolare che sostituirà la precedente.
- Le credenziali e le autorizzazioni di acceso sono gestite attraverso un sistema unico di Identity Management che provvede anche all'automatica disattivazione in corrispondenza della cessazione del rapporto di lavoro e o trasferimento ad altra unità organizzativa
- L'Istituto ha effettuato nel corso degli ultimi anni diversi interventi di formazione connessi agli aspetti riguardanti il trattamento dei dati sia in ambito amministrativo che statistico. Nel corso del 2019 gli attuari del Coordinamento statistico hanno partecipato al seminario dal titolo "Anti-Corruzione e Privacy".
- È stato redatto, ai sensi del Regolamento UE 2016/679, il Registro dei trattamenti relativo alle attività svolte dal Coordinamento statistico.

- L'Istituto non aderisce a codici di condotta o a meccanismi di certificazione, tuttavia adotta, attualizzandole, le linee guida dettate dal Garante. Il conferimento dell'incarico di responsabile è operato secondo le norme dettate dal Garante, in caso di ricorso a ditte esterne nella fase di assegnazione dell'attività la DC Appalti effettua il conferimento secondo i criteri riportati nell'articolo 28 del Regolamento UE 2016/679.
- Nei locali in cui sono posti server e banche dati avviene la registrazione degli accessi anche mediante riconoscimento biometrico, appositamente autorizzato dal Garante (a partire da ottobre 2019).
- L'informativa agli interessati è effettuata sul sito dell'Inps, mediante la modulistica e presso le sedi operative.
- Nel caso di contitolarità del trattamento sono stati sottoscritti accordi con il contitolare ai sensi dell'articolo 26 del Regolamento UE 2016/679.
- Per garantire l'esercizio dei diritti degli interessati è stata istituita una casella di posta elettronica dedicata insieme all'informativa che riporta la procedura da seguire per questioni relative al trattamento dei dati personali.
- In caso di utilizzo di supporti cartacei sono previste misure specifiche descritte nell'allegato 2 della circolare n. 123 del 2015 (allegato 3).
- Con particolare riferimento ad alcune categorie di dati sensibili, gli stessi vengono trattati solo attraverso tecniche di pseudonimizzazione in modo da consentire il trattamento necessario alle finalità istituzionali e allo stesso tempo garantirne la riservatezza per eventuali trattamenti di carattere statistico.

MISURE TECNICHE

- L'Istituto adotta un sistema di autenticazione basato su credenziali personali che prevedono le seguenti misure:
  - Regole di composizione della password di lunghezza minima di 8 caratteri e che contengano almeno una lettera, un numero e un carattere speciale;
  - Cambio della password ogni 3 mesi
  - Non utilizzabile nessuna delle ultime 3 password utilizzate.
  - Blocco automatico della postazione se non utilizzata per oltre 10 min
- Sono adottate misure per garantire la sicurezza della postazione di lavoro, come prescritto nel Disciplinare per l'utilizzo degli strumenti informatici reso disponibile dalla Direzione informatica tra cui:
  - Antimalware con application control
  - Sandbox anti APT
  - Gli utenti non sono amministratori delle postazioni di lavoro
  - Sistema di distribuzione automatica degli aggiornamenti del sistema e delle applicazioni
- Adozione di Intrusion Prevention Systems, antispam, motori multipli antimalware sulla posta elettronica, sistema di protezione della navigazione internet mediante antimalware e contentfiltering
- Adozione di meccanismi di pseudonimizzazione sui dati più sensibili
- Sono adottate misure per garantire la qualità e la correttezza dei dati sia a livello amministrativo sia a livello statistico.
- È adottato un sistema di monitoraggio e segnalazione degli incidenti, degli eventi anomali e delle violazioni, nel rispetto di quanto indicato nel Regolamento UE 2016/679 attraverso un IncidentResponseenadPreventrion Team.
- Il sistema informativo è distribuito su 3 datacenter: 2 datacenter per garantire la continuità operativa (business continuity) e 1 datacenter di disaster recovery per garantire il ripristino in seguito ad eventi catastrofici sui datacenter primari. I dati sono dunque replicati tra i 3 datacenter oltre ad esse archiviati su supporti durevoli attraverso appositi sistemi di backup
- I contratti di fornitura e manutenzione hardware prevedono specifici adempimenti per i fornitori riguardo alla distruzione sicura dei supporti di memorizzazione;
- Nella trasmissione dei dati con soggetti esterni si adottano canali di trasmissione sicuri (SFTP, HTTPS, …) o, laddove il conferimento debba avvenire su supporti removibili, si provvede a crittografare i dati.

Istituto Superiore di Formazione e Ricerca per i Trasporti – ISFORT

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)

Isfort, inottemperanza al Regolamento UE 2016/679, ha effettuato la DPIA, procedendo al monitoraggio delle proprie attività istituzionali di ricerca e formazione.

L'Istituto precisa che il trattamento dei dati personali, connessi agli adempimenti contabili e amministrativi, avviene su proprio server e tutte le attività informatiche collegate avvengono al proprio interno. I dati raccolti per le attività ordinarie sono dati anagrafici, dati amministrativi, dati contrattuali, con la sola eccezione dei dati sensibili di natura medica, raccolti e gestiti ai fini della gestione del personale, che sono trattati e conservati presso il medico incaricato.

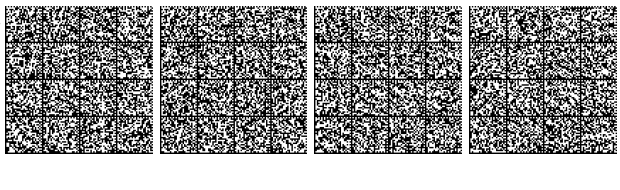
Per la attività *nell'ambito dell'area ricerca l'Istituto non raccoglie categorie particolari di dati ma esclusivamente dati personali non sensibili*. La raccolta e il trattamento dati di ricerca avviene esclusivamente attraverso soggetti specializzati in indagini e ricerche di mercato, finalizzati alla stesura dei rapporti annuali Audimob e altre ricerche istituzionali.

La verifica delle modalità di raccolta e trattamento dati nell'ambito delle predette indagini statistiche ha consentito di escludere che in tali attività istituzionali si svolgano trattamenti di dati personali e, a maggior ragione, di categorie particolari di dati come specificato dal Regolamento UE 2016/679.

L'Isfort, infatti, affida la raccolta dei dati utili alle proprie indagini statistiche a soggetti terzi, con specifichi incarichi, che tra le clausole espresse prevedono l'impegno a fornire all'Istituto i risultati di ciascuna indagine *in forma di microdati o aggregazioni di dati, in ogni caso esclusivamente anonimi e non riconducibili in alcun modo a persone fisiche*. I predetti incarichi prevedono, altresì, che a tale riguardo le agenzie incaricate si siano conformate alle previsioni del Regolamento UE 2016/679 – GDPR e che di ciò diano atto nell'accettazione degli incarichi.

L'Ente ha ritenuto, quindi, di designare quale *Responsabile del trattamento di dati personali*, con competenza sulle attività di ordinaria amministrazione e sulle attività dell'area ricerca, direttamente il *Titolare del trattamento, nella persona del proprio Direttore Generale pro tempore*.

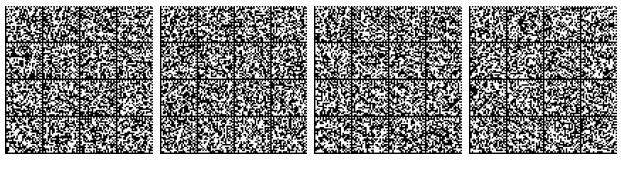
Quale addetti al trattamento dati personali dell'Ente, inclusa l'area ricerca ed esclusa l'area formazione, sono state designate 2 idonee risorse, con specifico incarico e istruzioni.



Diversa è la situazione relativa ai dati raccolti per le *attività di formazione regolata in ambito ANSF*, relativamente ai corsi per Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario, in conformità alle Linee Guida ANSF e alla Convenzione con Trenitalia S.p.A. del 19 ottobre 2017.
Detta formazione è erogata da Isfort per il tramite del proprio Centro di Formazione, come Centro riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie, che consentono di organizzare corsi per il rilascio della Licenza europea per la condotta dei treni.
Isfort ha ritenuto di effettuare, quindi, la valutazione dell'impatto dei trattamento previsti sulla protezione dei dati personali (DPIA) in applicazione del disposto della sezione 3 e degli artt. 27 e 35 del Regolamento UE 2016/679 – GDPR, e con particolare riferimento all'art. 9, comma 2, lettera d, del citato Regolamento, esclusivamente su detta area di formazione regolata in quanto solo in essa sono si effettuano trattamenti di categorie particolari di dati personali finalizzati dell'inserimento dei candidati nei corsi di cui in precedenza.
Nell'ambito del predetto processo di valutazione si è effettuata:

- la contestuale mappatura dei trattamenti effettuati dal Titolare
- la valutazione del rischio privacy
- la conduzione della DPIA per i soli trattamenti individuati come potenzialmente rischiosi
- la definizione dei trattamenti individuati da notificare al garante della Privacy
- la predisposizione del Registro dei rischi Privacy

In conseguenza di quanto sopra Isfort ha designato quale *Responsabile del trattamento dei dati personali del Centro di Formazione, il Direttore pro tempore del Centro***,** conferendo specifico incarico e idonee istruzioni.
Quale addetto al trattamento dati personali del Centro di Formazione, è stata designata idonea risorsa con specifico incarico e istruzioni.
Altre risorse effettuano, per la propria parte di competenza, trattamenti di dati del Centro di Formazione, di volta in volta individuate con specifiche lettere di incarico e istruzioni.
A sovrintendere le attività della Isfort in ambito informatico per il trattamento dati personali, è stata designata, idonea risorsa quale Responsabile della sicurezza dei sistemi informativi, con specifica lettera di incarico e istruzioni.
Da ultimo Isfort ha ritenuto di procedere a nomina del Responsabile della Protezione dei Dati (RPD/DPO), il cui atto di nomina è allegato al DPIA, con collegata comunicazione di legge al Garante della Privacy.
- Gestione delle autorizzazioni all'accesso ai dati
La gestione delle autorizzazioni di accesso avviene a seguito di idonee lettere di incarico e collegate istruzioni agli addetti da parte del Titolare del Trattamento.
- Interventi posti in essere per la formazione del personale
Nella predisposizione della DPIA, la modalità degli interventi è stata fortemente incentrata sul principio della responsabilizzazione e condivisione dei principi e delle procedure di protezione dei dati personali (cd. accountability principle). In ragione di ciò sono state portate a conoscenza di tutti gli incaricati, in primis e del resto della struttura, le informazioni e i nuovi principi che regolano le politiche di accountability approvate da Isfort e contestualmente gli incaricati sono stati edotti sui "rischi individuati e sui modi per prevenire i danni".
Per tutto il personale è stata organizzata una iniziativa di responsabilizzazione e condivisione dei principi e delle procedure di protezione dei dati personali, unitamente alla illustrazione delle funzioni, compiti e mansioni attribuiti dall'Istituto, agli addetti.
In sintesi i contenuti dell'informativa sono stati: panoramica delle vigenti disposizioni di legge; disposizioni legislative in tema di tutela dei dati e criminalità informatica; analisi delle norme in materia di protezione dei dati personali con particolare riferimento al Regolamento UE 2016/679 – GDPR; analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato; panoramica sugli adempimenti ex Regolamento UE 2016/679 – GDPR: notificazione, rapporti con gli interessati, rapporti con il Garante; l'attività dell'Ufficio del Garante della Privacy; misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi; prevenzione e contenimento del danno; strumenti di protezione hardware e software (in particolare antivirus e misure antihacker); contenitori di sicurezza, sistemi anti-intrusione, importanza e modalità di realizzazione delle operazioni di backup.
Agli addetti al trattamento, con specifiche comunicazioni di incarico, da parte del Titolare del Trattamento, sono state date precise istruzioni su funzioni, compiti, con riferimento sia alle norme che alle disposizioni interne del Manuale della Qualità, richiedendo la più scrupolosa osservanza delle informazioni e delle disposizioni impartite in relazione alle funzioni delegate. Le istruzioni agli addetti hanno precisato modalità di raccolta e trattamento dati personali sia senza l'uso di strumenti elettronici, ovvero raccolta e trattamento dati personali in modalità cartacea, fotocopiatura/ scansione con la finalità di trattamento autorizzato; modalità di raccolta e trattamento se si utilizza uno strumento elettronico (pc fisso, mobile, cellulare, supporti rimovibili) con sistema di autenticazione informatica e credenziali d'autenticazione abilitate dal Responsabile Sistema Informativo, su delega del Titolare del Trattamento.
Coerentemente con lo sviluppo delle attività di Isfort che comportino trattamento di dati personali, con l'evoluzione degli strumenti tecnici adottati dall'Istituto e/o con l'insorgere di nuove disposizioni legislative in materia, si provvederà ad aggiornare detta informativa, anche per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici
La DPIA è stata predisposta a seguito di puntuale monitoraggio di tutte le attività aziendali al fine di identificare ove si effettuano trattamenti di dati personali. Ne è derivata la stesura del Registro dei trattamenti, ai sensi dell'art.30, commi 1 e 2 del Regolamento Europeo (EU) 2016, 679, con particolare riferimento all'Area di trattamento Direzione Formazione Attività Sicurezza Ferroviaria, ove come meglio specificato in precedenza, avvengono trattamenti di categorie particolari di dati. È stata prevista la verifica delle misure adottate ogni sei mesi, ponendo l'attenzione a: verifica della efficacia delle misure di anti-intrusione adottate; corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati; previsione della disattivazione dei codici di accesso non utilizzati per più di sei mesi; aggiornamento dei dispositivi antivirus, dei programmi software che trattano i dati personali; integrità dei dati e delle loro copie di backup; sicurezza della conservazione dei documenti cartacei; accertamento della distruzione dei supporti magnetici non più essere riutilizzati; accertamento del livello di formazione degli incaricati; previsioni di sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda. Di queste verifiche sarà redatto un verbale che verrà allegato al documento programmatico sulla sicurezza.
- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
La società non aderisce a specifici codici di condotta. Si annota, altresì, che, con il fine di dare all'Istituto un complesso di governance societaria efficace, soprattutto in termini di vigilanza sull'applicazione dei principi di buona gestione aziendale sia nei riguardi degli utenti e committenti dei servizi sia degli stakeholders, la società si è dotata di un Sistema di Gestione per la Qualità (SGQ) sottoponendo a certificazione tutti i processi di gestione del prodotto e dei servizi ai clienti col fine di migliorarne continuativamente la qualità. Al termine



del processo di certificazione è stato redatto il Manuale della Qualità (MQ) con lo scopo di descrivere l'organizzazione e le attività operative per realizzare la Qualità secondo i punti della normativa UNI EN ISO 9001:2015 e le proprie modalità gestionali.
L'Ente ha ritenuto, quindi, di designare quale Responsabile del trattamento di dati personali, con competenza sulle attività di ordinaria amministrazione e sulle attività dell'area ricerca, direttamente il Titolare del trattamento, nella persona del proprio Direttore Generale pro tempore.
In quanto all'area formazione dell'azienda, come anzi detto, ove si effettuano trattamenti di categorie particolari di dati personali, finalizzati dell'inserimento dei candidati nei corsi di formazione regolata in ambito ANSF, per Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario, Isfort ha designato quale Responsabile del trattamento dei dati personali del Centro di Formazione, il Direttore pro tempore del Centro, conferendo specifico incarico e idonee istruzioni.
Entrambi gli incaricati sono, dunque, interni all'azienda.
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi
L'accesso alla sede è protetto da porta blindata. La sede non è aperta al pubblico e gli esterni si ricevono solo per appuntamento. L'accesso alle risorse dati in formato elettronico, da parte degli incaricati, avviene solo tramite gli elaboratori protetti da login e password, che consentono il log degli accessi. A tutto il personale Isfort che utilizza le postazioni è stato assegnato un elaboratore tramite il quale potranno accedere agli archivi in formato elettronico su cui operare i trattamenti. Gli incaricati preposti alla custodia degli archivi e al trattamento delle categorie particolari di dati dell'area Centro di Formazione sono state attribuite licenze di accesso al sistema Dropbox, protetti da login e password. La gestione delle licenze è affidata pro tempore a una risorsa addetta trattamento dati Centro di Formazione, nominata per iscritto, dal Titolare del Trattamento. Detto incaricato è custode delle licenze Dropbox che consentono l'accesso e il trattamento di categorie particolari di dati dell'area Centro di Formazione. La lettera di nomina è presente nei Mansionari DPIA. È stato individuato e nominato per iscritto, dal Titolare del Trattamento, l'amministratore di sistema RSI a cui è stato affidato il compito di sovrintendere alle risorse dei sistemi operativi degli elaboratori e delle basi dati ISF. È compito del RSI, su indicazione del Titolare del Trattamento, disattivare i codici identificativi in caso di mancato utilizzo per un periodo superiore ai sei mesi. Lo stesso RSI potrà, su disposizione del Titolare del Trattamento, avere accesso al sistema Dropbox, ove questo si rendesse necessario. La lettera di nomina dell'amministratore di sistema è presente nei Mansionari Privacy.
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")
La società adotta due modalità di conferimento delle informazioni ex articolo 13 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati"). Relativamente agli obblighi riferiti al trattamento di dati non sensibili la società comunica il conferimento delle succitate informazioni, integralmente, attraverso il proprio sito e, in forma sintetica, in calce alle e-mail inviate. Relativamente agli obblighi riferiti al trattamento di categorie particolari di dati personali, finalizzati dell'inserimento dei candidati nei corsi di formazione regolata in ambito ANSF, per Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario, acquisiti dalla società tramite iscrizione degli interessati, Isfort comunica il conferimento delle succitate informazioni attraverso idonea informativa. Detta informativa contiene tutti gli elementi richiesti dal citato art. 13 della norma europea e viene consegnata contestualmente alla domanda di iscrizione, e se ne richiede la sottoscrizione da parte degli interessati. Relativamente al conferimento delle informazioni ex articolo 14 del Regolamento (UE) n. 2016/679 Isfort precisa che per quanto attiene alla attività *nell'ambito dell'area ricerca l'Istituto non raccoglie categorie particolari di dati ma esclusivamente dati personali non sensibili*. La raccolta e il trattamento dati di ricerca avviene esclusivamente *attraverso soggetti specializzati in indagini e ricerche di mercato*, finalizzati alla stesura dei rapporti annuali Audimob e altre ricerche istituzionali. Si ribadisce, peraltro, che la società affidando la raccolta dei dati utili alle proprie indagini statistiche a soggetti terzi, con specifichi incarichi, che tra le clausole espresse prevedono l'impegno a fornire all'Istituto i risultati di ciascuna indagine *in forma di microdati o aggregazioni di dati, in ogni caso esclusivamente anonimi e non riconducibili in alcun modo a persone fisiche* non ha necessità di predisporre specifiche modalità di conferimento delle informazioni a norma del citato art. 14 non avendo alcun dato personale dei soggetti interessati. I predetti incarichi alle agenzie di ricerca prevedono, altresì, che dette agenzie incaricate si conformino alle previsioni del Regolamento UE 2016/679 – GDPR e che di ciò diano atto nell'accettazione degli incarichi.
- In caso di contitolarità del trattamento, sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679
L'Ente designato quale Responsabile del trattamento di dati personali, con competenza sulle attività di ordinaria amministrazione e sulle attività dell'area ricerca, direttamente il Titolare del trattamento, nella persona del proprio Direttore Generale pro tempore e quale il Responsabile del trattamento dei dati personali del Centro di Formazione, il Direttore pro tempore del Centro, conferendo specifico incarico e idonee istruzioni. Da ultimo Isfort ha ritenuto di procedere a nomina del Responsabile della Protezione dei Dati (RPD/DPO), il cui atto di nomina è allegato al DPIA, con collegata comunicazione di legge al Garante della Privacy.
- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati
Nell'ambito della informativa condivisa con tutti gli incaricati sono state fornite specifiche istruzioni in merito alla obbligatorietà di garantire l'esercizio dei diritti degli interessati. Diritti, peraltro, ribaditi nelle comunicazioni dell'azienda di cui agli obblighi ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati").
- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei
Gli archivi delle categorie particolari di dati trattati nell'area Centro di Formazione, su supporto cartaceo, sono posizionati in una stanza specifica, utilizzando degli armadi aventi una sezione a scaffali (per i supporti contenenti dati comuni) ed una munita di sportelli con serratura (per i supporti contenenti categorie particolari di dati personali). All'archivio cartaceo possono accedere solo i diretti incaricati, in quanto gli archivi sono vigilati dal personale preposto a tale servizio. Solo gli incaricati al trattamento di tali dati prelevano i documenti necessari per il trattamento per il tempo necessario a tale operazione, dopo di che hanno istruzioni di riporli nel sopraccitato luogo preposto alla loro conservazione, sotto la supervisione degli incaricati alla custodia dell'archivio. È compito dell'incaricato che preleva i documenti garantire che questi siano rinchiusi, sotto chiave, in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro.
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati
Come descritto in precedenza la società non effettua trattamenti di dati di soggetti vulnerabili. Le categorie particolari di dati personali trattati nell'area Centro di Formazione non riguardano soggetti vulnerabili o minorenni. I dati personali trattati nell'area Ricerca sono i risultati di ciascuna indagine *in forma di microdati o aggregazioni di dati, in ogni caso esclusivamente anonimi e non riconducibili in alcun modo a persone fisiche.*

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi
È stato attribuito un codice identificativo univoco (USER ID) a ciascun incaricato/utente Isfort per accedere al terminale assegnatogli. Gli incaricati preposti alla custodia degli archivi e al trattamento delle categorie particolari di dati del Centro di Formazione sono state attribuite licenze di accesso al sistema Dropbox, protetti da login e password. La gestione delle licenze è affidata a addetto, nominato per iscritto, dal

Titolare del Trattamento, quale custode delle licenze Dropbox che consentono l'accesso e il trattamento di categorie particolari di dati dell'area Formazione, unica in cui si ribadisce, sono trattate categorie particolari di dati personali. Il sistema Dropbox conserva in memoria tutti i log di accesso. Il codice di accesso all'area Dropbox dedicata sarà disattivato nel caso l'incaricato/utente perderà la qualità che consentiva l'accesso al terminale o quando tale codice è rimasto inutilizzato per un periodo superiore ai sei mesi.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Si rinvia a quanto già rappresentato al precedente punto "registrazione degli accessi delle persone nei locali".

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

A seguito di monitoraggio delle attività dell'azienda, ai fini della redazione della DPIA, avuto riguardo dei trattamenti descritti in precedenza, si sono valutate non necessarie misure e tecniche di cifratura e pseudonimizzazione.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

Si rinvia a quanto già rappresentato al precedente punto "adozione di specifiche misure in presenza di categorie vulnerabili".

- Adozione di misure per garantire la qualità e la correttezza dei dati

Come già rappresentato sono stati individuati e nominati per iscritto gli incaricati preposti alla custodia degli archivi e al trattamento di tutti i dati personali trattati in azienda, ivi inclusi gli addetti incaricati al trattamento di categorie particolari di dati del Centro di Formazione. Agli incaricati, congiuntamente alla lettera di nomina, sono state indicate le norme operative e di sicurezza a cui attenersi.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

Le risorse incaricate n.q. di Responsabile del trattamento di dati personali, con competenza sulle attività di ordinaria amministrazione e sulle attività dell'area Ricerca e con competenza sul Centro di Formazione, hanno ricevuto, nell'ambito dello specifico incarico, idonee istruzioni di mettere in atto, tutte le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione degli scopi statutari, ai sensi degli artt. 32 e 33 del Regolamento.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

I medesimi Responsabili del Trattamento hanno ricevuto istruzioni specifiche di adottare tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti; di informare il Titolare del trattamento e il DPO, senza ingiustificato ritardo, e comunque non oltre le 72 ore dal momento in cui si venga a conoscenza (art. 33 del GDPR), di eventuali violazioni dei dati personali (*data breach*) adottando, di concerto con gli stessi, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente. Viene richiesto, altresì, di predisporre e aggiornare un registro che dettagli, in caso di eventuali *data breach*, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate.

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

È stata implementata una procedura di cancellazione sicura dei dati a seguito di dismissione di apparecchiature elettroniche. I supporti magnetici, cartacei o di altro genere, verranno riutilizzati solo se i dati memorizzati in precedenza potranno essere eliminati in maniera sicura, altrimenti verranno distrutti.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

Si rinvia a quanto già rappresentato nei precedenti punti in merito alla sicurezza delle modalità di trattamento dei dati personali.

Istituto di servizi per il mercato agricolo alimentare - (Ismea)

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (Titolare – responsabili – incaricati);
- Gestione delle autorizzazioni all'accesso ai dati;
- Interventi posti in essere per la formazione del personale;- comunicazioni informative al personale;
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679;
- Controlli interni periodici;
- Adesione a codici di condotta;
- Conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto;
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi;
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati").

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di misure per garantire la qualità e la correttezza dei dati (backup – firewall – accessi controllati);
- Adozione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno del ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Istituto Superiore per la Protezione e la Ricerca Ambientale - ISPRA

I lavori ISPRA presenti nel Programma statistico nazionale 2020-2022 che trattano dati personali sono due:

- APA-00001 - Produzione, recupero, trattamento e smaltimento di rifiuti urbani, speciali e pericolosi;
- APA-00012 - Inventario delle emissioni in atmosfera.

Tra questi non sono compresi lavori che trattano "categorie particolari di dati" (relativi all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche e all'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) di cui all'articolo 9 del Reg. n. 2016/679/UE, nonché dati personali relativi a condanne penali e reati, di cui all'art. 10 del medesimo Regolamento.

MISURE ORGANIZZATIVE

Per quanto riguarda il lavoro *APA-00001 - Produzione, recupero, trattamento e smaltimento di rifiuti urbani, speciali e pericolosi*, le attività relative ai dati personali prevedono:
- acquisizione dei tracciati multi record *(Archivio amministrativo "MUD – Comunicazione annale al catasto rifiuti")* forniti dalla società Ecocerved (partecipata Unioncamere), contenenti i dati identificativi e di contatto delle ditte individuali e dei rappresentati legali degli operatori economici obbligati alla presentazione della dichiarazione MUD;
- costruzione, con cadenza periodica, delle "banche dati" attraverso il travaso dei tracciati multirecord di Unioncamere in formato MS Access utilizzabile da ISPRA e dal SNPA;
- fornitura delle "banche dati" alle singole Agenzie del SNPA per finalità statistiche (dato ambientale) e per finalità ispettive sul territorio (dato personale e ambientale);
- conservazione e fornitura dei dati ambientali e personali per ottemperare a specifiche richieste dell'autorità giudiziaria per le finalità di legge.

Il trattamento dei dati da parte di ISPRA avviene sia per finalità istituzionali (Art. 2-ter D.Lgs. n. 196/2003 e s.m.i.) ovvero per ottemperare agli obblighi di comunicazione nei confronti delle istituzioni nazionali ed europee come previsti dalla normativa vigente, sia per finalità di ricerca scientifica e statistica.
I soggetti interessati dal trattamento sono le - Ditte individuali e i Rappresentanti legali delle imprese tenute alla presentazione della dichiarazione del Modello Unico di Dichiarazione ambientale (MUD) ai sensi dell'articolo 189 del d.lgs. n. 152/2006;
I principali riferimenti normativi relativi all'attività sopra descritta sono a livello nazionale: art 189. D.Lgs. 152/2006, legge 132/2016; e a livello europeo: Reg. 2150/2002/CE; dir. 98/2008/CE, dec. 2000/532/CE dir. 2000/53/CE, dir. 2012/99/UE, dir. 94/62/CE, dir. 99/31/CE, dir. 2006/66/CE.
I dati in questione, vengono cancellati 12 mesi dopo l'acquisizione, al termine dei quali vengono pseudonimizzati e conservati per 5 anni per ottemperare a eventuali richieste dell'Autorità giudiziaria.
Tra le misure organizzative adottate, si segnalano: la formazione del personale coinvolto, le istruzioni generali per la sicurezza nel trattamento di cui alla Disposizione ISPRA. n.2019-1404/DG e la nomina soggetti autorizzati.

Per quanto riguarda il lavoro *APA-00012 - Inventario delle emissioni in atmosfera* le attività relative ai dati personali prevedono:
- acquisizione dei dati da ISTAT su supporto elettronico (CD-ROM) e/o tramite download da DG-STAT (Ufficio di Statistica SISTAN) e trasmissione degli stessi a VAL-ATM ai fini della elaborazione dei dati di produzione ai quali sono associati i dati amministrativi e gestionali delle ditte individuali e aziende produttive nei settori industriali (ASIA) e agricoli (SPA, Censimento Agricoltura);
- selezione dei dati di interesse per la realizzazione dell'inventario con esclusione dei dati amministrativi e gestionali che non sono di interesse nell'ambito della realizzazione dell'inventario delle emissioni.

Il trattamento dei dati da parte di ISPRA avviene sia per finalità istituzionali ovvero per ottemperare all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (Art. 2-ter D.Lgs. n. 196/2003 e s.m.i.), sia per finalità di ricerca scientifica e statistica.
I soggetti interessati dal trattamento sono le - Ditte individuali e i Rappresentanti legali delle aziende nonché gli Iscritti in albi ed elenchi.
I principali riferimenti normativi relativi all'attività sopra descritta sono il D.Lgs. 30/2013 Art.42 comma 4, D.Lgs. n. 322 del 1989
Tra le misure organizzative adottate, si segnalano: la formazione del personale coinvolto, le istruzioni generali per la sicurezza nel trattamento di cui alla Disposizione ISPRA. n.2019-1404/DG e la nomina soggetti autorizzati.

MISURE TECNICHE

Per quanto riguarda il lavoro *APA-00001 - Produzione, recupero, trattamento e smaltimento di rifiuti urbani, speciali e pericolosi,* relativamente alle misure di sicurezza tecnica si segnalano l'utilizzo di Antivirus, Autenticazione, Autorizzazione, *Business continuity, Firewall*, *Intrusiondetection*, Pseudonimizzazione.
L'ubicazione dei supporti di memorizzazione sono rappresentati dai personal computer delle postazioni di lavoro del personale coinvolto e da appositi server. I PC sono i dispositivi di accesso a questi dati e la tipologia di accesso è rappresentato da una copia fisica del materiale del DataBase, in remoto sul server.
L'attività di trattamento "APA-00001 - Produzione, recupero, trattamento e smaltimento di rifiuti urbani, speciali e pericolosi" sopra descritta è stata altresì inserita all'interno del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento UE 2016/679, tenuto dall'ISPRA mediante un applicativo interno creato ad hoc, e sono previste attività di monitoraggio e aggiornamenti interni periodici.

Per quanto riguarda il lavoro *APA-00012 Inventario delle emissioni in atmosfera***,** relativamente alle misure di sicurezza tecnica si segnalano l'utilizzo di Antivirus, Accesso controllato, Armadi chiusi, Autenticazione, *Firewall.*
L'ubicazione dei supporti di memorizzazione sono rappresentati dai personal computer delle postazioni di lavoro del personale coinvolto, e dai rispettivi armadi debitamente chiusi. I PC sono i dispositivi di accesso a questi dati e la tipologia di accesso è rappresentato dall'accesso ai dati da desktop tramite password.
L'attività di trattamento "APA-00012 Inventario delle emissioni in atmosfera" sopra descritta è stata altresì inserita all'interno del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento UE 2016/679, tenuto dall'ISPRA mediante un applicativo interno creato ad hoc, e sono previste attività di monitoraggio e aggiornamenti interni periodici.

Istituto superiore di sanità - ISS

Nell'ambito del PSN 2020-2022 l'ISS è titolare di 27 lavori statistici in cui si svolgono trattamenti di dati personali.
In questa nota vengono descritte sinteticamente le principali misure organizzative e tecniche che vengono adottate in ISS affinché i predetti trattamenti siano svolti seguendo le normative vigenti in tema di protezione dati.

MISURE ORGANIZZATIVE

L'ISS è articolato in 31 strutture tecnico scientifiche ed amministrative nelle quali si svolge un totale di circa 200 trattamenti di dai personali.

Il Titolare, rappresentante legale dell'Istituzione (attualmente il Presidente, già Commissario Straordinario, Prof. Silvio Brusaferro) ha individuato, ai sensi dell'art.2 – *quaterdecies* del Decreto Legislativo 30/6/2003, n. 196, cd Codice Privacy, come modificato dal Decreto Legislativo 10/8/2018, n.101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento Generale per la Protezione dei Dati, UE 2016/679, d'ora in poi denotato con RGPD), su indicazione dei Direttori delle predette strutture, con provvedimento Commissariale (Decreto n.13/2019) approvato dal Consiglio di Amministrazione dell'ISS, i soggetti autorizzati a ciascuno dei trattamenti (incaricati).

Si prevede di procedere a breve, sempre ai sensi del predetto articolo, all'individuazione da parte del Titolare dei soggetti designati a svolgere su sua delega una serie di funzioni inerenti al rispetto della normativa vigente in tema di protezione dati; tali designati saranno individuati nelle figure che dirigono le strutture tecnico scientifiche ed amministrative dell'ISS (Direttori di Dipartimenti, Centri, Servizi Tecnico-Scientifici, Direzione Generale, Direzioni Amministrative Centrali).

Per la *formazione del personale* sono stati messe in atto varie attività:

- per favorire la diffusione della cultura della protezione dati nel personale dell'ISS è stato richiesto a ciascun responsabile delle predette strutture di indicare due unità che fungano da "referenti/persone di contatto" per il DPO e per i colleghi che intendono avere informazioni sulla tematica del trattamento dei dati personali; tali unità di personale sono state individuate già prima dell'entrata in vigore del RGPD;
- prima e dopo l'entrata in vigore del RGPD sono stati organizzati e tenuti in ISS da parte del DPO e di componenti del Gruppo di Lavoro per la Protezione Dati, alcuni seminari rivolti ai "referenti", dedicati alle generalità del RGPD e ai concetti principali (Dati Personali, Trattamenti, Registro dei Trattamenti, DPO ecc..)
- subito dopo la loro designazione, gli incaricati dei trattamenti hanno seguito due corsi on-line messi a disposizione dal Servizio Informatico dell'ISS dedicati al RGPD, acquisiti senza ulteriore esborso di danaro da parte dell'ISS, essendo ricompresi in un "pacchetto" che riguarda la sicurezza informatica; il superamento di tali corsi ha dato luogo al rilascio di un attestato.

- Il sito sulla protezione dati

prima dell'entrata in vigore del RGPD è stato appositamente disegnato dal DPO e messo in linea il sito https://protezionedati.iss.it che ha Sezioni riguardanti: Generalità sul RGPD, Definizioni, il Registro dei Trattamenti, le Informative e la Sezione FAQ, che contiene una *check list* particolarmente consigliata prima di avviare uno studio in cui si prevede di trattare dati personali; il sito viene dinamicamente aggiornato di nuovi contenuti.

- Registro dei Trattamenti

Seguendo le priorità da attuarsi prima dell'entrata in vigore del RGPD, comunicate dal Garante alle Amministrazioni Pubbliche, si è provveduto ad elaborare il Registro dei Trattamenti; esso contiene le informazioni indicate nell'art. 30 del RGPD, in particolare: denominazione del trattamento, finalità, presupposti giuridici, sintetica descrizione dei soggetti a cui i dati si riferiscono e dei dati medesimi, elencazione di eventuali identificativi diretti, dati di mappatura fisica dei dati trattati. Il Registro, di cui esiste sia copia elettronica che cartacea, è stato realizzato mediante un'applicazione sviluppata *in-house* (a costo zero) e che si trova nella Intranet dell'ISS; esso è predisposto per essere dinamicamente aggiornato a cura del personale che in ciascuna struttura è stato individuato come referente per la protezione dati.

- Responsabile Esterno

È stato predisposto un modello per il conferimento da parte dell'ISS dell'incarico di responsabile esterno del trattamento, secondo quanto specificato dall'art. 28 e considerando 81 del RGPD; tale modello deve essere compilato da parte delle società/enti esterni che effettuano trattamenti per conto del Titolare.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

Il Data Center è dotato di un sistema di controllo degli accessi ai locali, la procedura prevede: tesserino identificativo, tastierino numerico, badge differenziato (per personale interno, per fornitori o per visitatori). Inoltre, l'accesso al Data Center è sempre accompagnato da personale tecnico autorizzato.

- Informative

È stato predisposto e reso disponibile sul sito un Modello per la redazione dell'Informativa agli interessati, secondo quando indicato dagli artt. 13 e 14 del RGPD.

- Esercizio dei diritti degli interessati

Nell'informativa vi è una parte apposita dedicata ai diritti degli interessati che include l'indicazione delle modalità con cui esercitarli; tali indicazioni sono contenute anche nel sito.

- Adozione di specifiche misure per la custodia di dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei.

Nei casi (limitati) in cui disposizioni di legge prescrivano che i dati debbano essere conservati su supporto cartaceo, i plichi sono custoditi in armadi blindati di sicurezza con chiusura a combinazione (del tipo delle casseforti) o con chiave, per i quali combinazione o chiave è nella responsabilità degli incaricati del trattamento; tali armadi di sicurezza vengono custoditi a loro volta in locali chiusi a chiave, in possesso del predetto personale.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

Il sistema di autenticazione è basato su tecnologia Microsoft Active Directory, in particolare

Il protocollo standard LDAP (Lightweight Directory Access Protocol) è usato per l'interrogazione e la modifica di una base di dati centralizzato contenente, in forma gerarchica, tutte le informazioni del dominio di rete iss.it relativamente ad autenticazioni ed accesso ai servizi IT; Le operazioni effettuate dall'utente, durante il processo di autenticazione, sono tracciate in file di log

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

La piattaforma Antivirus Kaspersky gestisce la sicurezza di circa 3.000 endpoint con supporto multipiattaforma (PC, Mac, iOS e Android), tra i quali anche i server e i sistemi di storage centralizzati presenti sull'infrastruttura di rete ISS. I sistemi operativi di tutti i computer presenti sulla rete Local Area Network (LAN) dell'ISS sono gestiti utilizzando la piattaforma software Microsoft Systems Management Server (SMS). SMS è utilizzato per l'amministrazione dei sistemi, essa consente il controllo da remoto delle postazioni di lavoro e dei server, la gestione delle patch, la distribuzione del software, l'inventario dell'hardware e del software in uso.

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

La sicurezza perimetrale della infrastruttura di rete è protetta da un cluster di due next-generation firewall (NGFW) Check Point con banda passante a 10Gbps e con servizi di sicurezza, per la prevenzione degli attacchi informatici, detti zero-day che non vengono intercettati dal sistema di antivirus. I NGFW dell'ISS includono le funzioni tipiche dei firewall tradizionali come il filtraggio dei pacchetti, la conversione di indirizzi di rete e di porte (NAT), l'ispezione stateful e il supporto alla gestione delle reti private virtuali (VPN), effettuano ispezioni più

approfondite rispetto a quelle eseguite dai firewall di prima e seconda generazione, controllando i payload dei pacchetti e le firme corrispondenti ad attività dannose, come possibili attacchi sfruttabili e malware.
È in corso un progetto che prevede la cifratura di tutti i dischi delle postazioni fisiche di lavoro.
- Data Breach
Per quanto riguarda il Data Breach, è stata inviata a tutti i direttori delle strutture tecnico scientifiche ed amministrative una Circolare del Direttore Generale dell'ISS che, al fine di provvedere tempestivamente agli obblighi di cui agli art. 33 e 34 del RGPD, relativi alla violazione dei dati personali (c.d. "*data breach*"), nella fase di prima attuazione del quadro normativo fornisce indicazioni al riguardo. È attualmente in corso di implementazione una procedura per il monitoraggio e la segnalazione di episodi di *data breach*.
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)
Per garantire la sicurezza dei dati presenti nei database centrali, in termini di affidabilità e di disponibilità, il sistema informatico è stato progettato nel seguente modo: un cluster di database server con tre stadi di conservazione del dato.
Nel primo stadio viene conservato il dato in linea implementato attraverso un array di dischi RAID (Redundant Array of Independent Disks). Il cluster garantisce la disponibilità del dato mentre l'affidabilità è assicurata dalla configurazione dell'array di dischi al livello RAID 5 con disco hot-spare per la sostituzione immediata di un disco in caso di guasto.
Il secondo stadio consiste in un backup giornaliero dei dati del primo stadio su un array di dischi del file server di backup configurato al livello RAID 6 utilizzando il software Symantec BackUpExec.
Il terzo stadio consiste in una copia dei dati effettuata ogni notte su Microsoft Cloud Storage. In caso di perdita totale o parziale dei dati degli archivi gli stessi possono essere agevolmente ricostruiti e resi disponibili ricorrendo alla copia di back*M*up.
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche
La cancellazione dei dati avviene utilizzando strumenti software diversi, a seconda del Sistema Operativo interessato, che consentono di effettuare cancellazioni sicure. Nel caso in cui le apparecchiature elettroniche da sottoporre a smaltimento non siano più funzionanti, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi, si procede con la distruzione fisica.

Istituto Nazionale di statistica

Le misure tecniche e organizzative sono state individuate in conformità alle scelte di politica di sicurezza dei dati effettuate dall'Istituto. In particolare, ai fini del presente documento, sono di seguito riassunte le misure di sicurezza applicate ai trattamenti a fini statistici sia per la salvaguardia dei beni e delle risorse elaborative (messa in atto di condotte volte alla prevenzione e alla protezione da possibili incidenti di carattere fisico che riguardino le strumentazioni informatiche e le aree in cui sono ubicate), sia la salvaguardia dell'integrità, della disponibilità e della riservatezza dei dati (modalità di protezione dei dati in tutte le fasi del trattamento: acquisizione, elaborazione, archiviazione, conservazione e diffusione; protezione dei sistemi, delle reti e degli applicativi; assegnazione dei corrispondenti profili di autorizzazione). Rientrano in questo secondo ambito anche le operazioni di back-up e di ripristino dei dati e dei sistemi, nonché la prevenzione e la gestione degli incidenti informatici.

MISURE ORGANIZZATIVE
Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati ai sensi dell'art.2-quaterdecies del d.lgs. n. 196/2003e soggetti autorizzati a trattare i dati)
Per assolvere ai compiti che l'articolo 24 del Regolamento europeo n. 2016/679 riconosce in capo al titolare del trattamento dei dati personali, con delibere del Presidente dell'Istat, in conformità a quanto previsto dall'art. 24 del Regolamento di organizzazione dell'Istituto, sono stati attribuiti al Direttore Generale, ai Direttori di Dipartimento, ai Direttori delle Direzioni centrali, al Dirigente dell'Ufficio di Presidenza(Servizio UPR), al Presidente dell'OIV, al Responsabile della prevenzione della corruzione e della trasparenza, al Presidente del CUG, al Presidente dell'Ufficio collegiale per i procedimenti disciplinari e al Capo dell'Ufficio stampa(c.d. "designati al trattamento dei dati personali") specifici compiti e funzioni connessi al trattamento dei dati personali afferenti agli ambiti di rispettiva competenza, ivi compresi l'individuazione dei soggetti autorizzati a trattare i dati e il compito di fornire specifiche istruzioni sulle modalità di trattamento e sulle misure da adottare per garantire la protezione dei dati personali.

Gestione delle autorizzazioni all'accesso ai dati
Ogni soggetto designato al trattamento dei dati personali individua – nell'ambito della propria sfera di competenza – le persone autorizzate a trattare i dati mediante l'adozione di una *Delibera di incarico al trattamento dei dati personali* che definisce l'ambito di autorizzazione al trattamento dei dati stessi. E' prevista, inoltre, la verifica periodica della sussistenza delle condizioni per il mantenimento delle autorizzazioni al trattamento dei dati personali e, nel caso esse non sussistano, la revoca delle stesse.

Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
La designazione di tali figure e l'individuazione delle relative funzioni viene formalizzata con appositi atti sottoscritti dai designati al trattamento dei dati personali competenti per materia. I soggetti esterni designati quali *Responsabili del trattamento* sono tenuti al rispetto delle vigenti disposizioni normative e delle istruzioni impartite dall'Istat, in conformità all'art. 28 del Regolamento europeo n. 2016/679

Interventi posti in essere per la formazione del personale
All'atto dell'assunzione presso Istat, oltre a presentare la mission, i compiti e l'organizzazione dell'Istat e del SISTAN, sono effettuate presentazioni e seminari che trattano la diffusione della cultura della sicurezza, della riservatezza e della protezione dei dati.
Nell'offerta formativa rivolta al personale, il medesimo tema è trattato all'interno di iniziative formative sia di natura metodologica sia di apprendimento organizzativo (ad esempio nei corsi sulla qualità del dato statistico o sul risk management). L'offerta formativa, infine, è completata anche con la partecipazione ai corsi SNA in materia di protezione dei dati personali.

Adesione a regole di settore
L'Istituto nazionale di statistica, nello svolgimento delle proprie attività, opera nel rispetto delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale*, nonché del *Codice delle statistiche europee* e della *Carta europea dei ricercatori*. In via generale, i dipendenti dell'Istituto sono altresì tenuti al rispetto delle disposizioni previste nel *Codice di comportamento dell'Istituto nazionale di statistica*.

Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

L'accesso fisico all'Istituto è regolato attraverso l'utilizzo di badge personali con foto e firma per tutti i dipendenti, un sistema di videocamere a circuito chiuso e una guardiania presidiata. Per i visitatori e i consulenti esterni è previsto l'accesso previa consegna di un documento di riconoscimento e contatto con l'ufficio cui è diretto il visitatore. Ogni visitatore esterno è intestato al nominativo di un dipendente dell'Istituto che giustifica la necessità dell'accesso e firma il foglio della sua presenza. L'accesso alle aree riservate e alla cd. "sala CED" è autorizzato al solo personale formalmente incaricato, i cui badge siano stati preventivamente abilitati. L'accesso è consentito tramite l'utilizzo del badge, sia in ingresso che in uscita, attraverso doppie porte allarmate e videosorvegliate. È presente un sistema di videocamere anche all'interno della sala macchine.

Modalità di conferimento delle informazioni ai sensi degli articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")
Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte dell'Istituto con modalità differenziate in relazione alle tecniche d'indagine utilizzate. In caso di indagini dirette, che prevedono l'acquisizione dei dati direttamente presso gli interessati, viene loro recapitata una lettera informativa del Presidente dell'Istituto nella quale sono descritte sia le finalità del trattamento, sia le modalità in cui questo avviene, sia la possibilità che i dati rilevati possano essere utilizzati anche per ulteriori trattamenti statistici, nonché l'obbligatorietà o meno del conferimento dei dati; l'informativa è resa anche oralmente nel caso di intervista, faccia a faccia o telefonica, effettuata da un intervistatore. Nei casi in cui i dati siano rilevati presso soggetti terzi e non sia agevole contattare gli interessati, l'informativa a questi ultimi viene resa attraverso il Programma statistico nazionale (PSN), l'atto di programmazione della statistica pubblica in cui sono descritte le caratteristiche di ciascun trattamento effettuato nell'ambito dei lavori statistici in esso inclusi, approvato con decreto del Presidente della Repubblica e pubblicato in Gazzetta Ufficiale.

Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati
L'Istat garantisce l'esercizio dei diritti degli interessati come previsto agli articoli 15 e ss. del Regolamento europeo 2016/679 e in conformità alle disposizioni dell'articolo 89 del medesimo Regolamento, dell'art. 6-bis, comma 8, del decreto legislativo n. 322/1989 e dell'art. 11 delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale*. Per l'esercizio dei propri diritti ciascun interessato può contattare il responsabile della protezione dei dati dell'Istat all'indirizzo di posta elettronica responsabileprotezionedati@istat.it.

MISURE TECNICHE

Sistema di autenticazione individuale degli utenti e tracciamento degli accessi
L'accesso alle infrastrutture tecnologiche dell'Istituto necessita di credenziali individuali fornite ad ogni dipendente al momento dell'assunzione, con rinnovo obbligatorio. Ogni accesso è tracciato e conservato per un periodo minimo di tre mesi.

Adozione di sistemi perimetrali di controllo
L'Istituto è dotato di un sistema di sicurezza perimetrale di tipo firewall per proteggere la rete locale da Internet. Il sistema firewall analizza le richieste di accesso da/per la rete esterna ed effettua controlli di sicurezza sul traffico della rete. Per fornire servizi all'esterno senza compromettere la sicurezza della rete interna, sono definite diverse zone utilizzate da specifiche applicazioni. I DB server Oracle presentano istanze distinte per i dati accessibili solo dalla rete interna e per i dati che vengono diffusi su Internet tramite gli application server. I firewall effettuano inoltre un controllo del traffico di rete per la rilevazione di anomalie e tentativi di intrusione. Agli apparati di tipo firewall sono affiancati i Web Application Firewall (WAF), dispositivi specializzati per la protezione delle applicazioni web.

Utilizzo di tecniche di pseudonimizzazione
I dati personali provenienti da fonti amministrative o da rilevazioni statistiche vengono sottoposti dall'Istat a procedure di pseudonimizzazione nella fase immediatamente successiva la loro acquisizione e – in ogni caso – prima di ogni forma di utilizzo a fini statistici, inclusa l'integrazione con altre informazioni presenti nei registri statistici. Le procedure di pseudonimizzazione prevedono dapprima la separazione dei dati identificativi diretti degli interessati dalle altre informazioni personali. Tali dati identificativi vengono successivamente trasformati in pseudonimi e solo questi ultimi sono riattribuiti alle altre informazioni personali, al fine di consentire di effettuare in modo coerente le necessarie operazioni di elaborazione statistica tra fonti diverse o tra una stessa fonte nel tempo. La tabella di raccordo tra gli identificativi diretti e i codici pseudonimizzati è conservata separatamente e utilizzata solo al fine di aggiornare il raccordo tra questi.

Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati
I dati rientranti nelle particolari categorie di cui all'articolo 9 del Regolamento europeo 2016/679 e i dati di cui all'articolo 10 del medesimo Regolamento sono trattati dall'Istituto per fini statistici con tecniche di cifratura o con l'utilizzo di codici identificativi o attuando altre soluzioni procedurali o organizzative che li rendono temporaneamente inintelligibili anche a chi è autorizzato a trattarli.

Adozione di strumenti per garantire la qualità e la correttezza dei dati
Un elevato livello di qualità delle statistiche ufficiali è da molti anni uno degli obiettivi che l'Istituto nazionale di statistica persegue regolarmente. Gli strumenti per la qualità sono stati predisposti dall'Istat coerentemente alla sua mission e in pieno accordo con il quadro di riferimento sviluppato da Eurostat per il Sistema statistico europeo. Si tratta, in particolare, delle *Linee guida per la qualità*, che contengono i principi per la progettazione, l'esecuzione e il controllo di qualità dei processi produttivi statistici e la descrizione dei metodi per garantire l'aderenza ai principi stessi. Esse sono lo standard di riferimento per la valutazione della qualità – sia di processo che di prodotto – dei processi condotti dall'Istat. Le *Linee guida*, infatti, sono utilizzate nelle procedure di audit e auto-valutazione statistico-metodologica. In un'ottica di trasparenza e per soddisfare le esigenze di diverse tipologie di utenti, la documentazione sulla qualità dei processi statistici dell'Istituto viene resa disponibile attraverso il *Sistema informativo sulla qualità (SIQual)*, dedicato alla navigazione dei metadati che descrivono ogni processo produttivo e le sue caratteristiche.

Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679
Le anomalie e gli incidenti aventi ripercussioni sul sistema informatico e sui livelli di sicurezza sono riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione al fine di minimizzarne l'impatto. L'individuazione di incidenti informatici in atto o avvenuti è resa possibile sia attraverso un apposito sistema di rilevazione degli attacchi installato nei punti critici della rete, sia attraverso l'accertamento di specifici eventi indicativi la cui rilevazione è affidata agli strumenti di monitoraggio, analisi dei Log e correlazione delle informazioni.

All'atto della constatazione di un incidente, in corso o avvenuto, ne viene data immediata comunicazione al personale tecnico informatico che provvede ad analizzare la gravità della situazione e a riportarla al dirigente del servizio e al direttore competente. I gestori dei sistemi informatici hanno la facoltà di bloccare l'accesso alle specifiche risorse implicate se viene rilevato che queste stiano rappresentando una minaccia effettiva o potenziale per la sicurezza del sistema o per il suo corretto funzionamento (intrusioni dall'esterno, diffusione di virus, invio massivo di spam, furto delle credenziali di accesso).
L'intervento può riguardare il blocco immediato e momentaneo di un'utenza di posta, di un PC, di una applicazione, di una banca dati, di un server e, se necessario, del collegamento da remoto alla risorsa; in una fase successiva, il detentore della risorsa viene messo al corrente dell'accaduto e delle specifiche del caso.

Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)
L'Istituto ha predisposto un piano per la configurazione in modalità ridondata dei sistemi di memorizzazione critici, Storage Area Network (SAN) e Network Attached Storage (NAS) con meccanismi di recupero automatico delle informazioni, e un piano di backup per tutti i sistemi server dell'ambiente distribuito e per le aree personali su server dei singoli utenti al fine di garantire il ripristino e la disponibilità dei dati.
È stato predisposto un piano di continuità operativa che permette all'Istituto di affrontare in modo organizzato ed efficiente le conseguenze di eventi imprevisti garantendo il ripristino dei servizi critici in tempi e con modalità che consentano di ridurne le conseguenze negative.

Modalità di cancellazione sicura dei dati in caso di dismissione di apparecchiature elettroniche
In attuazione della normativa vigente, al fine di riutilizzare, dismettere o rottamare apparecchiature elettroniche su cui siano stati memorizzati dati personali, il personale competente provvede alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino e, ove tale cancellazione non fosse realizzabile, alla distruzione del supporto. La cancellazione sicura delle informazioni è effettuata tramite la formattazione dei dispositivi o tramite l'impiego di programmi informatici che provvedono a sovrascrivere ripetutamente le aree precedentemente occupate dalle informazioni eliminate.
In caso di rottamazione di apparecchiature non più funzionanti, se non fosse possibile effettuare la cancellazione dei dati avvalendosi di software appropriato, tale cancellazione è effettuata tramite smagnetizzazione del dispositivo o procedure che comportino la distruzione fisica del supporto stesso.
Anche in caso di riutilizzo o dismissione di server su cui siano stati memorizzati dati personali, è obbligatorio provvedere alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino.

Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.
L'acquisizione di dati dall'esterno avviene esclusivamente attraverso canali di comunicazione cifrati, nella fattispecie HTTPS per l'acquisizione da archivi amministrativi su applicativi web dedicati (come nel caso di ARCAM) oppure FTPS su canali cifrati (a seconda dei casi utilizzando SSL/TLS o una VPN). Gli utenti possono accedere al sistema di acquisizione dati ARCAM o al server FTPS con utenza e password su canali cifrati. Le utenze sono nominative, rilasciate dall'Istat, e sono associate ai referenti formalmente incaricati del trasferimento dati presso le amministrazioni di appartenenza.

Archiviazione e conservazione dei dati
I dati personali trattati dall'Istituto con l'ausilio di strumenti elettronici sono archiviati e conservati in file o banche dati che risiedono su server gestiti a livello centrale. Non possono, pertanto, risiedere su singoli PC né possono essere memorizzati o duplicati su aree condivise pubbliche.

Ministero per i beni e le attività culturali e per il turismo

MISURE ORGANIZZATIVE
Nel Psn 2020-2022 è inserito il lavoro statistico "Sistema informativo sulle statistiche culturali" (codice PSN MBE-00012), nel quale vengono acquisiti i dati dal lavoro Istat "Indagine sui musei e le istituzioni similari" che tratta dati personali riferiti ai musei statali e non statali. È l'unico lavoro statistico che prevede il trattamento di dati personali.
- *Assetto organizzativo dell'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati*): l'Ufficio Statistica è inserito nel Servizio II della Direzione generale Bilancio del Ministero per i Beni e le attività culturali e per il turismo. Gli addetti all'Ufficio Statistica, in numero di 4, si occupano esclusivamente della funzione statistica, ad eccezione del responsabile che è anche il direttore del Servizio II, e come tali sono referenti del trattamento dei dati e sono i soli ad essere autorizzati all'accesso.
- *Adesione a codici di condotta e a meccanismi di certificazione*: i dipendenti dell'Ufficio di statistica sono stati informati e sono tenuti al rispetto delle disposizioni contenute nelle "Regole deontologiche per trattamenti a fini statistici e di ricerca scientifica effettuati nell'ambito del Sistema Statistico Nazionale" e nel "Codice di comportamento dei dipendenti pubblici".
- *Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi:* l'accesso fisico all'Ufficio Statistica è regolato attraverso l'utilizzo di badge personali. Per i visitatori è previsto l'accesso previa consegna di un documento di riconoscimento e contatto con l'Ufficio cui è diretto il visitatore, che ne firma il foglio di presenza. L'accesso ai locali del cosiddetto CED in cui sono posti i server e le banche dati e la protezione degli stessi è autorizzato al solo personale formalmente incaricato, con badge allo scopo abilitati.
- *Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati:* l'ufficio Statistica garantisce i diritti degli interessati che possono contattare il responsabile.

MISURE TECNICHE
- *Sistemi di autenticazione individuale degli utenti e tracciamento degli accessi*: le postazioni di lavoro dei dipendenti dell'Ufficio di Statistica, come di tutti i dipendenti del Ministero per i beni e le attività culturali e per il turismo, sono protette da un sistema di identificazione a due fattori con password da rinnovare periodicamente. Ogni accesso è tracciato e conservato per un certo periodo di tempo.
- *Adozione di sistemi perimetrali di controllo*: il Ministero è dotato di un sistema di sicurezza perimetrale di tipo firewall per proteggere la rete privata da internet. Il sistema analizza le richieste di accesso da e per la rete esterna ed effettua controlli di sicurezza sul traffico della rete.
- *Utilizzo di tecniche di pseudonimizzazione:* i dati personali provenienti dall'Indagine Istat sui musei e le istituzioni similari, non appena acquisiti, vengono sottoposti a procedure di pseudonimizzazione dapprima separando i codici identificativi diretti dalle altre informazioni personali e successivamente trasformando tali codici identificativi in pseudonimi, che vengono ricollegati alle altre informazioni personali. In questo

modo è possibile effettuare le elaborazioni tra fonti diverse o tra una stessa fonte nel tempo. La tabella di collegamento tra gli identificativi diretti e gli pseudonimi è conservata separatamente ed utilizzata solo a fini di aggiornamento.
- *Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto*): nel caso di incidente fisico o tecnico per le sale server sono attive misure antincendio e continuità operativa in caso di mancanza di corrente tramite l'impiego di gruppi di continuità (UPS) e gruppi elettrogeni; inoltre è attivo un sistema centralizzato di backup.
- *Modalità di cancellazione sicura dei dati in casi di dismissione delle apparecchiature elettroniche*: la cancellazione sicura dei dati è effettuata tramite la formattazione dei dispositivi.
- *Archiviazione e conservazione dei dati:* I dati personali sono archiviati e conservati in una banca dati che risiede su un server gestito a livello centrale.
- *Diffusione e comunicazione dei dati*: i dati personali, provenienti dal lavoro statistico dell'Istat "indagine sui musei e le istituzioni similari" sono diffusi in forma aggregata nel rispetto delle norme sulla Privacy e sul segreto statistico.

Ministero della difesa

Si descrivono, di seguito, le misure organizzative e tecniche adottate dall'Osservatorio Epidemiologico della Difesa nei trattamenti di dati personali. Le predette misure risultano altresì disciplinate:
- nell'ordine di servizio IGESAN n. 38 del 06 novembre 2018, prot. n. M_D SSMD REG2018 0175297 06-11-2018;
- nel registro delle attività di trattamento dell'OED;
- nelle misure minime di sicurezza relative al trattamento dei dati sensibili, da adottare per le attività dell'osservatorio epidemiologico della difesa (allegate e sottoscritte all'atto di nomina del rappresentante/autorizzato al trattamento dei dati personali).

MISURE ORGANIZZATIVE
- L'assetto organizzativo interno è strutturato in una titolarità del trattamento in capo all'Ispettore Generale della Sanità Militare, in un responsabile del trattamento, identificato nel Vice Ispettore ed in un Sub-responsabile, nel caso di specie il Direttore dell'OED; Il Referente per la Protezione dei dati personali è il Capo Coordinamento Generale; Il Direttore dell'OED procede all'atto di nomina dei soggetti autorizzati al trattamento, con dettaglio (scritto) dei compiti differenziati in relazione alla mansione svolta;
- Il personale autorizzato è stato edotto e formato anche tramite lezioni a cura dell'Ufficio Coordinamento Generale;
- È stato predisposto apposito registro delle attività di trattamento dell'OED, integrato in un analogo registro comprensivo di tutte le altre attività in capo ad IGESAN e custodito presso l'Ufficio Coordinamento Generale di detto Ispettorato.

MISURE TECNICHE
L'OED riceve, elabora ed archivia documentazione sanitaria e di servizio del personale militare e civile dell'Amministrazione della Difesa, per le finalità istituzionali assegnate di analisi epidemiologica ed eventuale diffusione verso Istituzioni militari e civili.
- *Raccolta dei dati:* il titolare, il responsabile ed il sub-responsabile del trattamento pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del "codice" e la tutela dei diritti degli interessati. Il personale incaricato della raccolta/trasferimento/archiviazione dei dati si attiene alle disposizioni e istruzioni ricevute. In particolare: a) assicura una particolare diligenza nella raccolta di dati sensibili o giudiziari e in generale cura la riservatezza dei dati trattati; b) provvede al corretto trasferimento dei dati raccolti, sia in formato cartaceo che elettronico, nel data-base dell'OED, rendendo il contenuto delle notifiche anonimo mediante la generazione di un codice identificativo univoco segreto, generato con un algoritmo informatico, a cura della Sezione Epidemiologia. Tutte le fasi successive di analisi dei dati a cura della Sezione Statistica verranno effettuate con il solo impiego del codice. Per particolari esigenze (p.es. richieste dell'autorità giudiziaria) sarà possibile risalire al nominativo dell'interessato mediante decodifica operata dal personale della Sezione Epidemiologia;
- *Conservazione dei dati:* I dati personali devono essere conservati per scopi statistici o scientifici anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati (relazioni allo SMD, Gabinetto del Ministro, interrogazioni parlamentari, richieste dell'autorità giudiziaria ecc.). In tali casi, i dati identificativi possono essere conservati fino a quando risultino necessari per: a) indagini continue e longitudinali; b) indagini di controllo, di qualità e di cope1iura; c) costituzione di archivi delle unità statistiche e di sistemi informativi; d) altri casi in cui ciò risulti essenziale e adeguatamente documentato per le finalità perseguite.
- *Misure di sicurezza:* L'OED non è aperto al pubblico. Chiunque, anche per motivi d'ufficio, debba entrare negli ambienti lavorativi dell'OED dovrà essere registrato presso il corpo di guardia di IGESAN (via S. Stefano Rotondo n. 4).
Gli Uffici dell'OED sono attualmente protetti da porta metallica dotata di serratura. L'uscita di sicurezza è apribile, con maniglia anti-panico, soltanto dall'interno. L'accesso ai locali è sorvegliato dal personale dell'OED. I singoli uffici sono dotati di serratura e vengono chiusi al termine delle attività quotidiane.
I dati personali e sensibili sono conservati in armadi, anche questi dotati di serrature e tenuti aperti solo per necessità di lavoro, per il tempo strettamente necessario. L'incaricato sa che deve tenere sulla scrivania soltanto pratiche in trattazione.
L'accesso ai computer è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione. La parola chiave, prevista dal sistema di autenticazione, è composta da almeno otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Per evitare usi fraudolenti, lo strumento elettronico lasciato inoperoso per oltre 5' va automaticamente in condizione di stand-by e per essere riavviato richiede una nuova digitazione della parola chiave.
Sono state implementate soluzioni tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
Sono vietati il trasferimento e la conservazione dei dati mediante l'uso di supporti rimovibili, se non per insuperabili motivi tecnici temporanei o se espressamente richiesti dall'Autorità Giudiziaria.
Sinteticamente, la raccolta dei dati sensibili avviene presso le strutture sanitarie a cura del personale sanitario. Pervengono all'OED con idonee modalità di protezione (busta chiusa con indicazioni specifiche, canali e sistemi informatici dedicati, criptati, etc.) e quindi archiviati in sede su supporto cartaceo e/o informatico. La custodia avviene in apposito mobilio dotato di serrature, in locali

accessibili esclusivamente al personale autorizzato. I dati custoditi in elaborati elettronici sono accessibili soltanto al personale in possesso di credenziali di autentificazione informatica (parola chiave riservata). Qualora il supporto informatico rimanga inattivo oltre 5' entra in blocco ed è necessario riavviarlo tramite la password riservata. I dati elettronici vengono anonimizzati ed il loro trattamento "in chiaro" avviene esclusivamente se i dati anonimi non consentono di svolgere le specifiche attività previste, comunque sempre secondo i limiti e le modalità indicate dalle normative di riferimento, nel rispetto dei principi di pertinenza e di non eccedenza.

Ministero dell'economia e delle finanze – Settore ex tesoro

- *Assetto organizzativo dell'attività di statistica del Ministero dell'Economia e delle Finanze* – Al fine di illustrare l'organizzazione dell'attività statistica e dei rapporti con l'ISTAT presso il Ministero dell'Economia e delle Finanza, e le conseguenti ricadute in termini di attività relativamente al trattamento di dati personali per finalità statistiche, si precisa che all'interno della struttura organizzativa del ministero, in base ai vigenti "*Regolamenti di organizzazione*", sono attualmente previsti due distinti uffici di statistica, retaggio della vecchia distinzione dei precedenti Ministeri del Tesoro e delle Finanze, che sono confluiti nell'attuale Ministero dell'Economia e delle Finanze.
L'ufficio di Statistica c.d. "*ex-Tesoro*" si occupa delle attività e dei progetti presenti nel SISTAN che fanno capo alle strutture organizzative dei Dipartimenti del Tesoro, della Ragioneria e degli Affari generali e personale del Ministero dell'Economia e delle Finanze. L'ufficio, inoltre, è responsabile delle attività comuni a carattere generale riferite al Ministero nel suo complesso, come nel caso delle attività riguardanti il"*Censimento delle Pubbliche amministrazioni*"nonché per altre "*Rilevazioni*" a carattere generale.
L'ufficio di Statistica c.d. "ex – Finanze" si occupa delle attività e dei progetti presenti nel SISTAN che fanno capo al Dipartimenti delle Finanze.
Entrambi gli uffici di Statistica si interfacciano con l'ISTAT per la gestione delle competenze relative alle attività statistiche delle rispettive organizzazioni dipartimentali di riferimento.
L'ufficio di Statistica "*ex – Tesoro*" e gli uffici dei dipartimenti che rappresenta e che gestiscono lavori e/o progetti presenti nel Psn, non raccolgono ed elaborano direttamente dati individuali sensibili.
La richiesta di dati personali da parte delle strutture organizzative del MEF (Dipartimenti / Direzioni /Uffici) a soggetti che ne dispongono (di regola all'ISTAT o all'ufficio di statistica del Dipartimento delle Finanze del medesimo ministero), per attività non collegate a progetti presenti nel Psn, avviene di regola, al fine elaborare statistiche nell'ambito dell'espletamento delle competenze istituzionali, come individuate e previste dalla normativa vigente.
In questi casi vengono poste in essere specifiche "misure tecnico – organizzative" volte a garantire l'ottemperanza di quanto previsto dalla normativa vigente in tema di privacy, che qui di seguito indicate:

MISURE ORGANIZZATIVE
- Definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento dei dati personali. In particolare viene distinto il ruolo dei soggetti designati a richiedere i dati personali ed i soggetti autorizzati a trattare ed elaborare i dati personali;
- Gestione dell'autorizzazione all'accesso ai dati;
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679;
- Vengono posti in essere interventi per la formazione del personale – di regola si tratta di corsi sulla privacy organizzati dalla Scuola Nazionale dell'Amministrazione (SNA) su richiesta della amministrazione nell'ambito dei piani di formazione.

MISURE TECNICHE
- Il trattamento di microdati personali viene esercitato esclusivamente dal responsabile per il trattamento dei dati;
- Sono utilizzate misure di autenticazione individuale per l'accesso ai dati: sono previste credenziali individuali per l'accesso ai dati;
- Sono utilizzate modalità di trasmissione dei dati all'interno del Ministero tali da garantire l'integrità, la disponibilità e la riservatezza delle informazioni;
- Sono previste modalità di cancellazione sicura dei dati in caso di dismissione dei PC (non ci sono server di dati sensibili).

Ministero dell'economia e delle finanze – Dipartimento finanze

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati);
- Gestione delle autorizzazioni all'accesso ai dati;
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici;
- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto.

MISURE TECNICHE
- Trattamento dei microdati personali esercitato esclusivamente dal "Responsabile Esterno per il Trattamento dei dati", tranne nel caso attività specificatamente indicate nel registro dei trattamenti;
- Sistema di tracciamento degli accessi al Datawarehouse di dati aggregati;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Utilizzo di tecniche di cifratura e/o pseudonimizzazione;
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati;
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Ministero delle politiche agricole

MISURE ORGANIZZATIVE - *Indagine PAC 00060 – Raccolta dati Acquacoltura ai sensi del Reg. CE 762/2008*
I dati raccolti dal CREA nell'ambito della raccolta dati acquacoltura non sono da considerarsi dati sensibili, essendo fornita esclusivamente la denominazione commerciale dell'impresa e la sua sede legale.
- *Gestione delle autorizzazioni all'accesso ai dati:* tutti i dati raccolti vengono caricati all'interno di una piattaforma cloud dedicata (http://www.acquaculturecrea.it/) e nel loro complesso sono accessibili soltanto al personale CREA specificatamente dedicato all'attività di elaborazione (Supervisori), mentre ciascun rilevatore, che raccoglie i dati direttamente presso le aziende, ha accesso alla piattaforma per il caricamento degli stessi e visualizza unicamente quelli da lui raccolti.
- *Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei*: non sono utilizzati supporti cartacei
- *Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati:* non sono presenti categorie vulnerabili di interessati ed i dati trattati non sono dati sensibili.

MISURE TECNICHE - *Indagine PAC 00060 – Raccolta dati Acquacoltura ai sensi del Reg. CE 762/2008)*
- *Sistema di autenticazione individuale degli utenti e tracciamento degli accessi:* l'accesso al sistema di raccolta ed immagazzinamento dei dati è consentito solo agli utenti autorizzati (rilevatori e supervisori), per mezzo di specifiche credenziali (ID e password), generate e gestite dai supervisori (CREA).
- *Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro:* tutte le postazioni individuali di lavoro sono dotate di computer con accesso personale tramite password.
- *Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati:* i dati grezzi raccolti dal CREA sulle produzioni dell'acquacoltura nazionale riguardano esclusivamente i nominativi commerciali di imprese e impianti, indirizzi delle sedi legali e produzioni di specie di pesci, molluschi, crostacei ed alghe, ma in nessun modo si raccolgono informazioni sugli operatori del settore. L'elaborazione dei dati per la distribuzione (invio Eurostat, FAO/GFCM) consiste in una aggregazione a livello regionale o per specie allevata e tali aggregati rappresentano il massimo livello di dettaglio di diffusione delle elaborazioni.
- *Adozione di misure per garantire la qualità e la correttezza dei dati:* controlli di routine automatici e manuali fatti al momento della digitalizzazione dei dati, al fine di prevenire possibili errori. L'applicativo specificatamente messo a punto per la raccolta dati in acquacoltura ha un sistema automatico per la prevenzione degli errori nell'inserimento dei dati che blocca il "work flow" se si inseriscono caratteri non consoni (es. lettere, caratteri speciali, ecc.)
- *Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto):* i dati sono immagazzinati su una piattaforma cloud realizzata esclusivamente per dati raccolti nell'ambito del Reg. CE 762/2008.
- *Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche*: i dati sono immagazzinati incloud.
- *Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni:* la trasmissione dei dati sia all'interno del CREA che all'esterno dell'Ente, avviene solo in modalità aggregata e nel rispetto delle norme di riservatezza sopra descritte. Dalla piattaforma cloud è possibile fare il download dei dati in formato .xml necessario per il caricamento sul sito EDAMIS (Eurostat). I dati sono caricati sul portale SIPAM della FAO-GFCM attraverso inserimento manuale.

Ministero dello sviluppo economico

MSE-00008 Indagine annuale sulla Grande distribuzione: Despecializzata (grandi magazzini, supermercati, ipermercati, minimercati); Specializzata (Grandi Superfici Specializzate)**.**

MISURE ORGANIZZATIVE
Il Ministero per lo Sviluppo Economico si è dotato di un proprio assetto organizzativo per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei diversi soggetti coinvolti in tale trattamento con la emanazione della direttiva del 28 gennaio 2020, a firma del Ministro Patuanelli.
La "Direttiva per la individuazione dei soggetti attraverso i quali il Ministero dello sviluppo economico esercita le funzioni di titolare del trattamento, ai sensi del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati" individua, come titolare del trattamento, il Ministero stesso che esercita tale funzione attraverso i soggetti individuati nell'art. 5: il Capo di Gabinetto, il Segretario Generale, i Direttori Generali competenti per materia, il titolare dell'OIV.
Inoltre è stato recentemente nominato il responsabile della protezione dei dati nella persona della dott.ssa Paola Picone.
Il Titolare del trattamento designa (art 9 della Direttiva) il responsabile del trattamento.

MISURE TECNICHE
La Direttiva 28 gennaio 2020 del Ministro Patuanelli prevede, all'art. 14, che il Segretario Generale, con il supporto del Responsabile della protezione dei dati e con il supporto informatico della Direzione Generale per le risorse, l'organizzazione, i sistemi informativi e il bilancio (DGROSIB), indichi le modalità operative per l'organizzazione del registro delle attività di trattamento.

Ministero della giustizia

Elementi informativi sulle misure tecniche ed organizzative adottate nei trattamenti dei dati personali per finalità statistiche nei lavori MGG-00119 *"Minori sottoposti a provvedimento penale in carico ai Servizi minorili del Dipartimento per la Giustizia minorile e di comunità"* e MGG-00120 *"Adulti in area penale esterna"*

MISURE ORGANIZZATIVE
I dati dei minorenni e giovani adulti dell'area penale in carico ai Servizi minorili sono gestiti attraverso il Sistema Informativo dei Servizi Minorili (SISM), che contiene tutti i dati del minore, relativi alla sua situazione personale e familiare, alla sua posizione giuridica, agli interventi trattamentali attuati dal personale socio-educativo e gli altri dati necessari ai fini della presa in carico.

Il sistema è su rete Intranet, cui si accede mediante credenziali individuali rilasciate dalla Direzione Generale dei Sistemi informativi (DGSIA) del Ministero in modalità ADN.
I dati gestionali sono inseriti nel sistema SISM dagli operatori dei Servizi minorili, secondo profili di accesso definiti in base alla tipologia di Servizio ed alla funzione svolta.
I dati e le applicazioni risiedono su server presso i CED della DGSIA.
I dati degli adulti in area penale esterna in carico agli Uffici di esecuzione penale esterna sono gestiti attraverso il sistema informativo PEGASO, che contiene i dati anagrafici dei soggetti in carico ed i dati relativi al tipo di misura o di indagine per cui i soggetti sono seguiti.
Il sistema è installato localmente nelle sedi degli Uffici e le credenziali di accesso sono rilasciate dal Direttore dell'Ufficio.
I dati gestionali sono inseriti nel sistema PEGASO dagli operatori e dagli assistenti sociali in servizio negli Uffici di esecuzione penale esterna, secondo profili di accesso definiti in base alla funzione svolta.
I dati e le applicazioni risiedono localmente presso i singoli Uffici.
Nell'ambito del Ministero della Giustizia, il trattamento a fini statistici dei dati derivanti dagli archivi gestionali del Dipartimento per la Giustizia minorile e di comunità è stato inserito, ai sensi Regolamento (EU) n.679/2016 e del Decreto Legislativo n. 101/2018 di adeguamento della normativa nazionale, nel Registro delle attività di trattamento, attualmente in fase di perfezionamento.
L'Amministrazione, per la sicurezza dei sistemi informatici, opera nell'ambito delle direttive fornite dalla DGSIA.

MISURE TECNICHE
Il sistema statistico acquisisce, direttamente dai sistemi gestionali, i soli dati utili ai fini statistici, con particolare riferimento alle caratteristiche personali dei soggetti, ai provvedimenti disposti dall'Autorità Giudiziaria, alle tipologie di reato.
Il sistema statistico non contiene gli identificativi diretti.
L'elaborazione dei dati avviene attraverso i cruscotti informativi statistici (CIS) realizzati con l'applicativo di Business Intelligence *QlikView*.
Le statistiche prodotte con l'applicativo *QlikView* sono elaborate sulla base dei dati gestionali del Sistema Informativo dei Servizi Minorili (SISM), aggiornati giornalmente e del sistema PEGASO, aggiornati ogni quindici giorni.
I cruscotti sono realizzati in modo da riconoscere l'utente che si collega ed assegnare allo stesso i diritti di visibilità sui dati in funzione delle politiche di sicurezza definite. In particolare, ciascun Centro per la Giustizia Minorile, Servizio minorile e Ufficio interdistrettuale di esecuzione penale esterna può accedere soltanto ai dati statistici di propria competenza. L'Amministrazione Centrale gestisce i suddetti profili di accesso ed il rilascio delle utenze.
I dati statistici sono pubblicati in forma aggregata attraverso raccolte di tavole e analisi statistiche, con approfondimenti tematici e analisi storiche e territoriali. Sono resi disponibili sul sito Internet del Ministero della Giustizia *www.giustizia.it* e sul sito Internet del Centro Europeo di Studi di Nisida, *www.centrostudinisida.it*.

Ministero dell'Istruzione, dell'Università e della Ricerca

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)
La gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento per il Ministero viene disciplinata da quanto disposto con la Direttiva del Ministro del 25 marzo 2019, n. 239 - Linee guida sui soggetti del processo di gestione della privacy del Ministero.
In conformità alle disposizioni in materia di trattamento dei dati personali, è stato designato tra i dipendenti dell'Amministrazione il responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento europeo n. 2016/679 (nomina AOOUFGAB - Ufficio del Gabinetto del MIUR Prot. n. 0000282 - 16/04/2018). Il RPD svolge le attività ad esso attribuite dall'art.39 del Regolamento con le garanzie di indipendenza e di autonomia previste dalle disposizioni normative vigenti.
Per assolvere ai compiti previsti dall'art.24 del Regolamento, la suddetta Direttiva n.239/2019 individua i soggetti mediante i quali il MIUR esercita le funzioni di Titolare del trattamento dei dati personali (Dir.239/19, art.2). Tali soggetti possono a loro volta nominare un Referente per la privacy come figura di supporto nelle funzioni di coordinamento e come punto di contatto con il Responsabile della protezione dati. Possono inoltre affidare specifici compiti e funzioni connessi al trattamento dei dati a dirigenti che da essi dipendono, designandoli espressamente (Dir.239/19, art.4).
- Gestione delle autorizzazioni all'accesso ai dati
Attraverso le prescrizioni della Direttiva del Ministro del 25 marzo 2019, n. 239 (art.5) sono individuati i soggetti autorizzati al trattamento dei dati tra i dirigenti degli uffici dirigenziali generali e non generali, il personale non dirigente in servizio ed il personale della scuola comandato nei limiti delle competenze attribuite all'Ufficio o alla struttura di appartenenza.
Dal punto di vista operativo, le autorizzazioni per l'accesso ai dati vengono gestite tramite l'adozione di procedure automatizzate di gestione delle credenziali per:

- registrare ed abilitare a specifici servizi tramite il portale SIDI del MIUR, i referenti che partecipano alle Rilevazioni previste dai progetti PSN dell'area istruzione (progetti PUI);
- registrare ed autorizzare online specifici referenti che partecipano alle Rilevazioni previste dai progetti PSN dell'area della formazione superiore (progetti MUR);

Con un sistema di gestione nominativo delle credenziali (active directory) vengono altresì gestite le autorizzazioni per l'accesso ai dati da parte dei soggetti autorizzati al trattamento che si trovano nelle sedi del Ministero.
- Gestione dei Responsabili del trattamento e delle terze parti
In caso di trattamento dei dati svolto da soggetti esterni per conto del MIUR, per quanto attiene al settore Scuola è stato nominato un Responsabile del trattamento attraverso atti formali di designazione ai sensi dell'art. 28 del Regolamento europeo. I soggetti esterni designati quali Responsabili del trattamento sono tenuti al rispetto delle indicazioni fornite dal MIUR (titolare del trattamento) e ad assicurare che le persone autorizzate al trattamento dei dati personali siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (Dir.239/19, art.7).
Per quanto attiene al settore Università, Afam e Ricerca la nomina è in corso di definizione.
- Interventi posti in essere per la formazione del personale

È stato avviato un piano di formazione attraverso corsi sulla privacy erogati in modalità E-learning sulla piattaforma Sidi del MIUR, al fine di far acquisire al personale un livello di conoscenza in materia di privacy adeguato al proprio ruolo.

- Monitoraggio e aggiornamento periodico del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679

Ai sensi dell'articolo 30 del Regolamento è stato istituito il Registro dei trattamenti di dati personali avviati dal Ministero ed è previsto l'aggiornamento nel caso di avvio di nuovi trattamenti o l'eventuale modifica dei trattamenti in essere. Nel registro sono descritte, per ciascun trattamento, la finalità, la tipologia dei dati (personali e/o non personali, rientranti nelle particolari categorie di cui all'art.9 del Regolamento europeo n. 679/2016), le strutture interne e/o esterne che effettuano o concorrono al trattamento, le caratteristiche delle banche dati utilizzate con la loro ubicazione fisica e gli estremi degli atti di autorizzazione al trattamento dei dati personali.

- Adesione a codici di condotta e a meccanismi di certificazione

Il MIUR avvia qualunque trattamento di dati personali in conformità alle disposizioni delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale, nonché nel rispetto del Codice delle statistiche europee. In via generale, i dipendenti del Ministero sono altresì tenuti al rispetto delle disposizioni previste nel Codice di condotta dell'Amministrazione e nel Codice di comportamento dei dipendenti pubblici.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

L'accesso fisico al Ministero è regolato attraverso l'utilizzo di badge personali con foto e firma per tutti i dipendenti, un sistema di videocamere a circuito chiuso e una guardiania presidiata. Per i visitatori e i consulenti esterni è previsto l'accesso previa consegna di un documento di riconoscimento e contatto con l'ufficio cui è diretto il visitatore. Compatibilmente con le "Misure minime di sicurezza ICT per le pubbliche amministrazioni dettate dall'AGID" l'accesso alla sala server interna al ministero è presidiato e limitato al solo personale preventivamente autorizzato; ogni ingresso viene registrato sul relativo registro degli accessi.

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte del MIUR attraverso l'Informativa ex art. 14 del Regolamento (UE) n. 2016/679 pubblicata sul sito del MIUR e nell'albo delle istituzioni scolastiche.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

Il MIUR garantisce l'esercizio dei diritti degli interessati come previsto agli artt.15 e ss. del Regolamento (UE) n. 2016/679 e in conformità alle disposizioni dell'art.89 del medesimo Regolamento, dell'art. 6-bis, c.8, del decreto legislativo n. 322/1989 e dell'art.11 delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale. Nelle informative ex art. 14 del Regolamento ("informazioni agli interessati") pubblicate sul sito del MIUR e nell'albo delle istituzioni scolastiche vengono indicati l'indirizzo postale del soggetto titolare del trattamento (direzione competente per la specifica rilevazione) e il recapito RPD come punti di contatto per l'esercizio dei diritti da parte degli interessati.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

L'accesso alle infrastrutture tecnologiche del Ministero necessita di credenziali individuali fornite ad ogni dipendente al momento dell'assunzione. Il servizio di autenticazione si basa sul principio che ogni utente che accede alle risorse del sistema deve essere univocamente identificato attraverso un codice unico nel sistema e strettamente associato ad una persona fisica, che ne è responsabile dell'uso. Il Login Server verifica le credenziali dell'utente: ottenuto l'accesso, tracciato nel sistema, l'utente può così accedere ai servizi/applicazioni in base ai suoi profili di abilitazione.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Le credenziali individuali sono gestite in modo centralizzato e sono oggetto di aggiornamento come tutti i software facenti parte della build standard certificata ed approvata dall'Amministrazione, compresi Antivirus, browsers, patch di sicurezza di Windows, ecc.

È previsto un controllo agli accessi fisici all'edificio (le cui attività di vigilanza sono gestite dal servizio di portineria che si avvale di un sistema di video sorveglianza) ed alle stanze (dotate di serratura).

- Adozione di sistemi perimetrali di controllo

Il Ministero è dotato di un sistema di sicurezza perimetrale di tipo firewall per proteggere la rete locale da Internet. Il sistema firewall analizza le richieste di accesso da/per la rete esterna ed effettua controlli di sicurezza sul traffico della rete. I firewall effettuano inoltre un controllo del traffico di rete per la rilevazione di anomalie e tentativi di intrusione.

- Utilizzo di tecniche di pseudonimizzazione

Nei progetti che prevedono l'utilizzo dei dati individuali provenienti da fonti amministrative vengono utilizzate tecniche di pseudonimizzazione per il trattamento dei dati, cheprevedono la separazione dei codici identificativi diretti degli interessati dalle altre informazioni personali. Tali codici identificativi vengono successivamente trasformati in pseudonimi e questi ultimi sono riattribuiti alle altre informazioni personali, al fine di consentire di effettuare in modo coerente le necessarie operazioni di elaborazione statistica tra fonti diverse o tra una stessa fonte nel tempo. La tabella di raccordo tra gli identificativi diretti e i codici pseudonimizzati è conservata separatamente ed utilizzata solo al fine di aggiornare il raccordo tra questi.

- Adozione di misure per garantire la qualità e la correttezza dei dati

Gli strumenti per la qualità dei dati del MIUR, con il supporto dell'Istat, sono ispirati allo standard di riferimento per la valutazione della qualità dei prodotti e dei processi rappresentato dalle Linee guida per la qualità sviluppate da Eurostat per il Sistema statistico europeo, che contengono i principi per la progettazione, l'esecuzione e il controllo di qualità dei processi produttivi statistici e la descrizione dei metodi per garantire l'aderenza ai principi stessi.

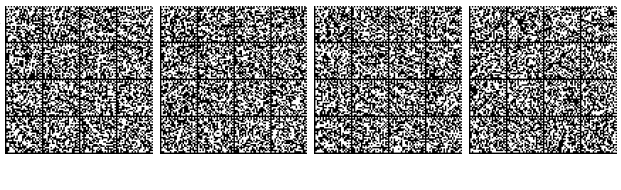
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

Le anomalie e gli incidenti aventi ripercussioni sul sistema informatico e sui livelli di sicurezza sono riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione al fine di minimizzarne l'impatto. All'atto della constatazione di un incidente, in corso o avvenuto, ne viene data immediata comunicazione al personale tecnico informatico che provvede ad analizzare la gravità della situazione e a riportarla al dirigente del servizio e al direttore competente. È inoltre previsto un piano di backup periodico sia delle banche dati che dei server al fine di garantire il ripristino e la disponibilità dei dati. Inoltre, al fine di garantire la continuità operativa, il Private Cloud del MIUR usufruisce di una soluzione di DisasterRecovery sul sito secondario dove è replicata la stessa configurazione logica presente nel sito primario.

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

In attuazione alla normativa vigente, al fine di riutilizzare, dismettere o rottamare apparecchiature elettroniche su cui siano stati memorizzati dati personali, il personale competente provvede alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni



È in corso di predisposizione un'area dedicata sicura per lo scambio di dati personali attraverso canali di comunicazione cifrati.
- Conservazione dei dati
I dati personali o individuali trattati dal MIUR con l'ausilio di strumenti elettronici sono conservati in file o banche dati che risiedono su server gestiti a livello centrale. La conservazione dei dati personali è necessaria per adempiere l'esecuzione di compiti di interesse pubblico e nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento a fini statistici nel rispetto delle garanzie di sicurezza e riservatezza.
- Diffusione e comunicazione dei dati
È prevista la diffusione dei soli dati sui quali siano stati effettuati i necessari controlli per garantirne la rispondenza alle norme sul segreto statistico e sulla riservatezza. I dati statistici prodotti sono diffusi solo in forma aggregata, in modo da non poter risalire all'identificazione degli interessati.

Ministero del lavoro

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)
In conformità alle disposizioni in materia di trattamento dei dati personali, tramite D.M. del 21 febbraio 2019, n. 21 è stato designato tra i dipendenti dell'Amministrazione un Responsabile della protezione dei dati il quale svolge, con le garanzie di indipendenza e di autonomia previste dalle disposizioni normative vigenti, le attività attribuitegli dall'art. 39 del Regolamento (UE) n. 2016/679.
Per assolvere ai compiti che l'articolo 24 del Regolamento europeo n. 2016/679 riconosce in capo al titolare del trattamento dei dati personali, si segnala, altresì, che con D.M. n. 37 del 10 aprile 2019, recante "*Direttiva per la individuazione dei soggetti tramite i quali il Ministero del lavoro e delle politiche sociali esercita le funzioni di titolare del trattamento, ai sensi del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", sono stati declinati i ruoli e le responsabilità in ordine agli adempimenti previsti in capo al Ministero del lavoro quale titolare del trattamento dei dati personali, nel complesso delle sue articolazioni organizzative. Nello specifico, tramite la menzionata Direttiva, il Capo di Gabinetto, i Capi degli Uffici di diretta collaborazione del Ministro, il Segretario Generale, i Direttori Generali e il Titolare dell'Organismo indipendente di valutazione della performance, sono stati individuati quali soggetti esercenti le funzioni di titolare del trattamento dei dati personali, ciascuno nel rispettivo ambito di competenza.
- Gestione delle autorizzazioni all'accesso ai dati
Gli esercenti le funzioni di titolare del trattamento sono chiamati, *inter alia*, a designare e a istruire, tramite appositi atti scritti, gli autorizzati al trattamento, i referenti privacy e i responsabili interni del trattamento dei dati. Ciascun soggetto esercente le funzioni di titolare del trattamento è chiamato a tenere un elenco aggiornato degli autorizzati che operano all'interno della propria sfera di competenza. Al di fuori di tale elenco, i dipendenti non destinatari di una formale designazione non devono svolgere operazioni di trattamento di dati e sono considerati, a tali fini pari a soggetti terzi, rispetto al titolare.
- Interventi posti in essere per la formazione del personale
Su indicazione del Responsabile della protezione dei dati del Ministero, sono state avviate le attività volte all'organizzazione della formazione in materia di privacy e data protection da parte della Direzione Generale dei sistemi informativi, dell'innovazione tecnologica, del monitoraggio dati e della comunicazione, tramite la rilevazione dei fabbisogni formativi per l'anno in corso. Attesa la situazione contingente che a causa dell'*emergenza Covid-19* impedisce, ad oggi, lo svolgimento di corsi di formazione in aula, la citata Direzione Generale ha provveduto all'acquisizione di una soluzione di formazione a distanza da somministrare al personale del Ministero. Nello specifico, da aprile 2020 tutto il personale del Ministero sarà coinvolto in un corso e-learning dedicato alla privacy e alla sicurezza informatica, mirato a innalzare il livello di conoscenza e sensibilità del personale verso la protezione dei dati trattati dall'Amministrazione.
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679
Il Ministero si è dotato di un Registro delle attività di trattamento dei dati personali svolte dall'Amministrazione. Il Registro delle attività di trattamento del Ministero è stato realizzato nel primo semestre del 2018, a seguito di un'attività di assessment. Nel secondo semestre 2018, su incarico del Responsabile della protezione dei dati (RPD) *pro-tempore*, e sotto il coordinamento della Direzione Generale dei sistemi informativi, dell'innovazione tecnologica, del monitoraggio dati e della comunicazione, è stato avviato un progetto volto a sistematizzare il registro delle attività di trattamento all'interno di un software, facilitandone, in tal modo, la tenuta e il suo costante aggiornamento. Le attività di implementazione dell'applicativo gestionale del registro sono state recentemente completate e si prevede una sua progressiva e graduale messa a sistema nell'anno in corso. In tale sede, il registro attualmente utilizzato sarà oggetto di una diffusa attività di aggiornamento e integrazione dei contenuti, con lo scopo estendere l'ambito di utilizzo dello stesso e renderlo uno strumento di gestione dei rischi e degli adempimenti in materia di tutela dei dati personali più agile ed efficace.
- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
Nelle ipotesi in cui l'Amministrazione ricorre a soggetti esterni per il trattamento dei dati, gli Uffici esercenti le funzioni di titolare del trattamento provvedono a regolare i rapporti con la terza parte e a definire i rispettivi perimetri di titolarità nel rispetto della normativa vigente, tramite contratto o altro atto giuridico, come espressamente previsto dall'art. 8 del D.M. n. 37 del 10 aprile 2019. A tal fine, con la collaborazione dell'assistenza tecnica, sono stati predisposti dei modelli di accordo ai sensi dell'art. 28 del Regolamento (UE) 2016/679, da impiegare come base per poi essere declinati sulla scorta delle singole fattispecie. A partire dal 2019, all'interno dei bandi di gara indetti dall'Amministrazione, ove necessario, sono inserite, come clausole standard di contratto, l'individuazione dell'aggiudicatario quale responsabile del trattamento.
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi
L'accesso fisico ai locali dell'Amministrazione è controllato attraverso la scansione di *QR code* personali per tutti i dipendenti, visitatori e consulenti esterni. Nello specifico, per i dipendenti e i consulenti esterni è previsto l'accesso tramite badge personale dotato di *QR code*; per i visitatori, l'accesso è consentito esclusivamente previa consegna di un documento di riconoscimento, un contatto diretto con l'ufficio cui è diretto il visitatore e il *QR code*. L'ingresso inoltre, è controllato mediante un sistema di videocamere a circuito chiuso e una guardiania presidiata.
L'accesso ai locali in cui sono collocati i server dell'Amministrazione è consentito esclusivamente al personale formalmente autorizzato, i cui badge siano stati preventivamente abilitati. L'accesso è consentito tramite l'utilizzo del badge, sia in ingresso che in uscita. È presente un sistema di videosorveglianza all'interno e all'esterno delle sale server.
- Modalità di conferimento delle informazioni ai sensi degli articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati da parte dell'Amministrazione. Il Ministero ha provveduto ad aggiornare le informative e i moduli di raccolta dei dati personali degli interessati – comprese le informative e i moduli online – al fine di renderli conformi alla normativa vigente in materia di trattamento di dati personali.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

Il Ministero garantisce l'esercizio dei diritti degli interessati come previsto agli articoli 15 e ss. del Regolamento (UE) n. 2016/679 e in conformità alle disposizioni dell'articolo 89 del medesimo Regolamento, dell'art. 6-bis, comma 8, del decreto legislativo n. 322/1989 e dell'art. 11 delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale*. Come chiarito all'interno di ciascuna informativa, per l'esercizio dei propri diritti ciascun interessato può contattare il responsabile della protezione dei dati all'indirizzo di posta elettronica gdpr@lavoro.gov.it.

- Predisposizione di un sistema di segnalazione di eventi che potrebbero generare una violazione di dati personali (data breach)

Il Ministero, tramite comunicazione del Responsabile della protezione dei dati *pro-tempore*, ha fornito al personale una serie di indicazioni comportamentali volte a prevenire la possibilità di perdita, alterazione, divulgazione, anche accidentale, di dati personali, nonché a evitare di tenere condotte che possano consentire l'accesso a soggetti non autorizzati a dati trasmessi, archiviati o altrimenti elaborati dall'Amministrazione. In tale sede il personale è stato, altresì, invitato a comunicare ogni possibile episodio che potrebbe dar luogo ad una violazione di dati personali. L'Ufficio del Responsabile della protezione dei dati ha, inoltre, messo a disposizione del personale un modulo volto ad agevolare la comunicazione di eventuali violazioni di dati personali, al fine agevolare una pronta risposta ed eventuale comunicazione della violazione all'Autorità Garante, come previsto dagli artt. 33 e 34 del Reg. (UE) 2016/679.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

L'accesso alle infrastrutture tecnologiche dell'Amministrazione necessita di credenziali individuali fornite ad ogni utente. In riferimento al sistema SISCO, ossia il Sistema Informativo Statistico delle Comunicazioni Obbligatorie, si segnala che l'accesso da parte degli utenti interni all'Amministrazione avviene in modalità *single sign on*, essendo il suddetto sistema integrato con il dominio. L'accesso da parte di utenti esterni all'Amministrazione prevede l'inserimento di credenziali e password univocamente assegnate. Per le utenze amministrative sono tracciati nei log sia i tentativi di accesso fallito che i tentativi di accesso andati a buon fine.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Per accedere alle postazioni fisiche di lavoro, ogni utente deve necessariamente autenticarsi al dominio, mediante l'inserimento di credenziali univocamente assegnate e soggette a scadenza periodica. Il sistema di autenticazione per tutti gli utenti obbliga l'utilizzo di password di autenticazioni "forti" che soddisfano requisiti di complessità.

- Adozione di sistemi perimetrali di controllo

L'Amministrazione ha attivato su tutte le postazioni fisiche di lavoro, pc portali e server Windows un sistema perimetrale di tipo *firewall* e *antimalware* per proteggere i sistemi dall'eventuale installazione, diffusione ed esecuzione di codice malevolo. Il sistema *firewall* è caratterizzato da regole inbound/outbound che permettono l'accesso a protocolli di rete ben definiti da sorgente a destinazione. Sono inoltre presenti sistemi di *Intrusion prevention* per controllare il traffico e le attività di sistema al fine di identificare l'esecuzione di codice non previsto.

Nei casi in cui si rendano necessarie operazioni di amministrazione remota di server, dispositivi di rete e analoghe apparecchiature, le stesse sono eseguite mediante connessioni protette, ossia protocolli criptati e intrinsecamente sicuri.

- Utilizzo di tecniche di anonimizzazione

I dati relativi alle comunicazioni obbligatorie (di seguito "CO") inviate dai datori di lavoro o nodi intermediari sono sottoposte dall'Amministrazione a procedure di anonimizzazione nella fase immediatamente successiva alla loro raccolta e prima di ogni forma di trattamento e conservazione del dato statistico (SISCO). I dati statistici prodotti dall'Amministrazione e messi a disposizione per finalità di ricerca si riferiscono ad un campione anonimo di individui dipendenti e parasubordinati, integrato da eventi di lavoro autonomo desunti dagli archivi Inps (file CICO: Campione Integrato delle Comunicazioni Obbligatorie). I file CICO, disponibili con cadenza trimestrale, sono protetti da password e gli enti di ricerca che presentano, tramite il portale *Cliclavoro* una richiesta corredata da un progetto di ricerca possono accedere a tali banche dati solo se in possesso delle credenziali di autenticazione per il download dei dati comunicati.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

I dati rientranti nelle particolari categorie di cui all'articolo 9 del Regolamento Europeo e i dati di cui all'articolo 10 del medesimo Regolamento sono trattati dall'Amministrazione attuando soluzioni procedurali o organizzative che li rendono temporaneamente intelligibili solo a chi è autorizzato a trattarli.

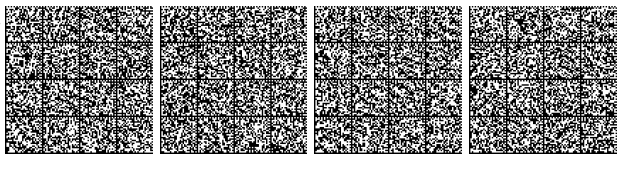
- Adozione di strumenti per garantire la qualità e la correttezza dei dati

Gli strumenti atti a garantire la qualità e la correttezza dei dati sono applicati per tutte le statistiche ufficiali dell'Amministrazione e in particolare durante l'intero processo di creazione della principale fonte informativa statistica detenuta dal Ministero del lavoro e delle politiche sociali, ossia il Sistema Informativo Statistico delle Comunicazioni Obbligatorie (SISCO). L'Amministrazione infatti, ha definito un livello minimo di controlli aggiuntivi per verificare la correttezza formale (es: verifica della compilazione dei dati obbligatori, formato dei campi, ecc.) e relazionale (es: controllo delle caratteristiche del lavoratore coinvolto nel rapporto di lavoro, controllo delle date di fine rapporto in caso di contratto a tempo determinato, ecc.) delle CO sin dal primo momento di acquisizione del dato, ossia quando sono trasmesse dai nodi di raccolta regionali verso il Nodo di Coordinamento Nazionale (NCN). Le CO che non superano i controlli tecnici del NCN vengono rinviate al nodo da cui provengono con il dettaglio dell'errore individuato. Tali CO dovranno essere corrette dal soggetto mittente e reinviate, con l'inizio del nuovo percorso di controllo sulle porte di domino del NCN. Nel processo di costruzione del SISCO, inoltre, sono implementati meccanismi di controllo e di eventuale correzione di alcune informazioni all'interno delle singole CO e meccanismi di controllo destinati a classificare ed escludere dalle successive elaborazioni statistiche CO con palesi errori e incongruenze.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

Le anomalie e gli incidenti aventi ripercussioni sul sistema informatico e sui livelli di sicurezza sono riconosciuti e gestiti attraverso sistemi di prevenzione, comunicazione e reazione al fine di minimizzarne l'impatto. L'individuazione di incidenti informatici in atto o avvenuti è resa possibile sia attraverso un apposito sistema di rilevazione degli attacchi installato nei punti critici della rete, sia attraverso l'accertamento di specifici eventi indicativi la cui rilevazione è affidata agli strumenti di monitoraggio e analisi dei *log*.

L'Amministrazione ha previsto procedure differenti a seconda della gravità degli incidenti; nello specifico, gli incidenti classificati come "lievi", ossia gli incidenti risolvibili con contromisure "locali" e /o incidenti che non comportano un fermo delle applicazioni per un periodo di tempo superiore rispetto a quello definito accettabile, sono gestiti mediante il processo di *incident management*; gli incidenti "gravi"



che determinano dei malfunzionamenti alle infrastrutture/funzionalità critiche sono gestiti con i processi intermedi di *Business Continuity Management* e infine, gli incidenti classificati come "estremi", che portano alla dichiarazione dello stato di "disastro" sono gestiti con i processi di *Business Continuity Management* e *Disaster Recovery*.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

Al fine di garantire la disponibilità e il ripristino dei dati in caso di necessità, l'Amministrazione effettua regolarmente operazioni di backup, la cui frequenza e modalità sono documentate in una procedura dedicata. Le copie di backup sono conservate su supporti non permanentemente accessibili onde evitare che eventuali attacchi possano coinvolgere anche le copie di sicurezza. I set di backup sono gestiti in doppia copia. Mensilmente è verificata l'utilizzabilità delle copie mediante prove di ripristino.

È stato predisposto un piano di continuità operativa che permette all'Amministrazione di affrontare in modo organizzato ed efficiente le conseguenze di eventi imprevisti garantendo il ripristino dei servizi critici in tempi e con modalità che consentano di ridurne le conseguenze negative.

- Modalità di cancellazione sicura dei dati in caso di dismissione di apparecchiature elettroniche

Al fine di riutilizzare, dismettere o rottamare apparecchiature elettroniche su cui siano stati memorizzati dati personali, il personale competente provvede alla loro preventiva cancellazione sicura in maniera da renderne impossibile il ripristino e, ove tale cancellazione non fosse realizzabile, alla distruzione del supporto. La cancellazione sicura delle informazioni è effettuata tramite la formattazione dei dispositivi o tramite l'impiego di programmi informatici che provvedono a sovrascrivere ripetutamente le aree precedentemente occupate dalle informazioni eliminate.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

L'acquisizione di dati dall'esterno avviene esclusivamente attraverso canali di comunicazione cifrati SSL. Gli utenti esterni all'Amministrazione possono accedere alle banche dati statistiche solo se sono in possesso di credenziali di autenticazione.

- Archiviazione e conservazione dei dati

I dati personali o individuali trattati dall'Amministrazione con l'ausilio di strumenti elettronici sono archiviati e conservati in file o banche dati che risiedono su server fisici e/o virtuali gestiti a livello centrale.

Ministero delle infrastrutture e dei trasporti

I dati personali relativi a lavori PSN di competenza di questa Amministrazione (ad esclusione di quelli che utilizzano informazioni riferite a persone giuridiche, enti o associazioni), riguardano:

- MIT-00029 - Implementazione di registri unici sui sinistri marittimi e sugli infortuni marittimi e portuali
- MIT-00010 - Immatricolazioni e passaggi di proprietà di autovetture
- MIT-00011 - Patenti in corso di validità e neopatentati

Premesso che il d.p.c.m. 11 febbraio 2014, n. 72, recante "Regolamento di organizzazione del Ministero delle Infrastrutture e dei Trasporti, ai sensi dell'articolo 2 del Decreto-Legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla Legge 7 agosto 2012, n. 135", pone in capo alla Direzione Generale per i Sistemi Informativi e Statistici le competenze in materia di gestione e sviluppo dei sistemi informativi trasversali, lasciando alle singole Strutture del Ministero delle Infrastrutture e dei Trasporti le competenze sui sistemi informativi verticali, si riportano di seguito le informazioni richieste, per come sono state comunicate dalle Strutture responsabili dei tre lavori PSN su citati.
In particolare:

- MIT-00029 - Implementazione di registri unici sui sinistri marittimi e sugli infortuni marittimi e portuali

(Titolare del lavoro: Direzione generale per la vigilanza sulle autorità portuali, le infrastrutture portuali ed il trasporto marittimo e per vie d'acqua interne del Ministero delle Infrastrutture e dei Trasporti)

MISURE ORGANIZZATIVE

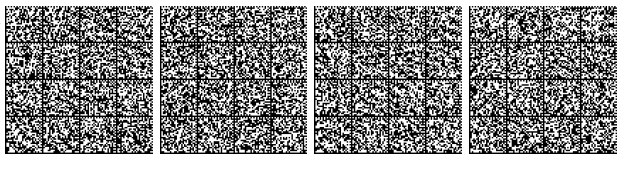
I dati personali utilizzati nello studio progettuale MIT-00029 sono trattati esclusivamente da dipendenti dell'Ufficio designati a tal fine. Tali dipendenti sono soggetti all'osservanza della norma generale contenuta nel DPR 16 aprile 2013, n. 62 "Regolamento recante codice di comportamento dei dipendenti pubblici", che prevede all'articolo 12, comma 5, che "Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Qualora non sia competente a provvedere in merito alla richiesta cura, sulla base delle disposizioni interne, che la stessa venga inoltrata all'ufficio competente della medesima amministrazione". Inoltre i dipendenti del ministero delle infrastrutture e dei trasporti sono tenuti all'osservanza delle disposizioni previste dal codice di comportamento adottato per lo stesso Ministero con DPCM n. 27315 del 26 settembre 2014, che all'art. 12, commi 5 e 6, dispone che "Il dipendente deve utilizzare i servizi telematici e telefonici dell'Ufficio, nel rispetto dei vincoli posti dall'Amministrazione" e "al dipendente è fatto divieto di diffondere e pubblicare, anche tramite social network, notizie e informazioni di cui sia a conoscenza per ragione del proprio ufficio", e all'art. 13, commi 3 e 4, prevede che "il dipendente … si astiene dal fornire ai mezzi di comunicazione qualunque informazione attinente il contesto organizzativo ovvero le attività d'ufficio, eccettuate quelle già pubblicate ai sensi della normativa vigente, al di fuori dei casi di previa autorizzazione" e "nel rispetto delle disposizioni di legge e regolamentari in materia di accesso e tutela e trattamento dei dati personali, il dipendente, nel rispondere a richieste di informazioni per via telefonica o a mezzo posta elettronica, si attiene alla seguente modalità di comportamento:

- ove le stesse non vertano su proprie competenze specifiche, indirizza tempestivamente il richiedente verso l'Ufficio per le relazioni con il pubblico o la struttura competente;
- se la richiesta rientra direttamente nelle proprie competenze, fornisce prontamente al soggetto direttamente interessato dal provvedimento le informazioni ed i chiarimenti non coperti da segreto d'ufficio, e, in ogni caso, informa sempre gli interessati della possibilità di avvalersi delle forme di accesso previste dalla legge e dai regolamenti dell'Amministrazione".

Inoltre gli accessi alle sedi ministeriali sono soggetti a registrazione e non è possibile accedere ai locali in cui sono posti i server e le banche dati senza previa autorizzazione degli Uffici competenti, e qualora ciò avvenga, è assicurata la presenza di un dipendente addetto a tali sistemi.

MISURE TECNICHE

I dati trattati sono archiviati in fogli MS-Excel, allocati in postazioni di lavoro munite di un sistema di autenticazione individuale dei dipendenti incaricati; inoltre è conservato un backup degli archivi in un'area virtuale.



La proprietà dei dati e la vigilanza sugli stessi sono del Ministero delle Infrastrutture e dei Trasporti. La qualità, le procedure e regole di archiviazione, aggiornamento e di conservazione, sono stati fissati con ordine di servizio della struttura interessata. I dati raccolti nell'ambito dello studio sono tutelati dal segreto statistico e sottoposti alle regole stabilite, a tutela della riservatezza, dal Reg. CE n. 322/97, dal D. Lgs 196/03. I medesimi dati possono essere utilizzati, anche per successivi trattamenti, esclusivamente per fini statistici dai Soggetti del Sistema statistico nazionale e possono essere comunicati per finalità di ricerca scientifica alle condizioni e secondo le modalità previste dal Codice di deontologia per i trattamenti di dati personali effettuati nell'ambito del Sistan. La loro diffusione avviene inoltre esclusivamente in forma aggregata in modo che non si possa risalire ai soggetti che li forniscono o ai quali si riferiscono (art. 9-D.Lgs 322/89).

- *MIT-00010- Immatricolazioni e passaggi di proprietà di autovetture (ex INF-00010)*
- *MIT-00011 - Patenti in corso di validità e neopatentati (ex INF-00011)*

(Titolare dei due lavori: Direzione Generale per la Motorizzazione del Ministero delle Infrastrutture e dei Trasporti)

MISURE ORGANIZZATIVE

I dati personali utilizzati sono trattati esclusivamente da dipendenti dell'Ufficio designati a tal fine nonché da membri autorizzati dell'RTI (Raggruppamento Temporaneo di Imprese) che gestisce in outsourcing il Sistema Informativo MCTC .

I dipendenti del Ministero preposti al trattamento dei dati sono soggetti all'osservanza della norma generale contenuta nel DPR 16 aprile 2013, n. 62 "Regolamento recante codice di comportamento dei dipendenti pubblici", che prevede all'articolo 12, comma 5, che "Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Qualora non sia competente a provvedere in merito alla richiesta cura, sulla base delle disposizioni interne, che la stessa venga inoltrata all'ufficio competente della medesima amministrazione". Inoltre i dipendenti del Ministero delle Infrastrutture e dei Trasporti sono tenuti all'osservanza delle disposizioni previste dal codice di comportamento adottato per lo stesso Ministero con DPCM n. 27315 del 26 settembre 2014, che all'art. 12, commi 5 e 6, dispone che "Il dipendente deve utilizzare i servizi telematici e telefonici dell'Ufficio, nel rispetto dei vincoli posti dall'Amministrazione" e "al dipendente è fatto divieto di diffondere e pubblicare, anche tramite social network, notizie e informazioni di cui sia a conoscenza per ragione del proprio ufficio", e all'art. 13, commi 3 e 4, prevede che "il dipendente … si astiene dal fornire ai mezzi di comunicazione qualunque informazione attinente il contesto organizzativo ovvero le attività d'ufficio, eccettuate quelle già pubblicate ai sensi della normativa vigente, al di fuori dei casi di previa autorizzazione.

Gli accessi alle sedi ministeriali sono soggetti a registrazione e non è possibile accedere ai locali in cui sono posti i server e le banche dati senza previa autorizzazione degli Uffici competenti, e qualora ciò avvenga, è assicurata la presenza di un dipendente addetto a tali sistemi.

MISURE TECNICHE

I dati finalizzati alla produzione di statistiche sono inseriti in un Datawarehouse, munito di un sistema di autenticazione individuale dei dipendenti incaricati e del personale autorizzato del Raggruppamento Temporaneo di Imprese che gestisce in outsourcing il Sistema informativo della Motorizzazione. Gli universi che costituiscono le basi dati del DWH sono conservati fisicamente negli stessi server blade che ospitano tutti gli altri dati del SIDT e sono quindi protetti da accessi non autorizzati da un sistema di firewall. Un primo livello di sicurezza è stabilito a livello di rete e permette l'accesso ai dati solo agli utenti che accedono dall'interno della rete stessa.

L'accesso alle funzionalità del DWH è poi consentito solo previa autenticazione individuale dei dipendenti del Dipartimento, Direzione Generale Motorizzazione, Centro Elaborazione Dati, deputati all'estrazione dei dati per finalità statistiche (o per indagini di polizia). Nello specifico alcune risorse del CED sono state dotate di Nulla Osta di Sicurezza (NOS) con qualifica "Riservatissimo/Nazionale"

I dati sono gestiti in modo da assicurare la protezione dei dati in essa contenuti seguendo le policy stabilite dal "Documento Programmatico sulla Sicurezza" formulato e mantenuto aggiornato annualmente dall'Amministrazione, coadiuvata dal RTI che gestisce il SiDT in outsourcing. Il documento descrive l'elenco dei trattamenti informatici svolti da RTI, i rischi di sicurezza associati a tali trattamenti e le misure minime di sicurezza implementate per mitigare tali rischi in accordo con il Piano Nazionale per la sicurezza ICT ed il Modello Organizzativo Nazionale per la Sicurezza ICT.

La proprietà dei dati e la vigilanza sugli stessi sono del Ministero delle Infrastrutture e dei Trasporti. I dati raccolti sono tutelati dal segreto statistico e sottoposti alle regole stabilite, a tutela della riservatezza, dal Reg. CE n. 322/97, dal D. Lgs 196/03. I medesimi dati possono essere utilizzati, anche per successivi trattamenti, esclusivamente per fini statistici dai Soggetti del Sistema Statistico Nazionale e possono essere comunicati per finalità di ricerca scientifica alle condizioni e secondo le modalità previste dal Codice di deontologia per i trattamenti di dati personali effettuati nell'ambito del Sistan. La loro diffusione avviene inoltre esclusivamente in forma aggregata in modo che non si possa risalire ai soggetti che li forniscono o ai quali si riferiscono (art. 9-D.Lgs. 322/89)

Ulteriori informazioni trasmesse dal CED della Motorizzazione

Di seguito sono descritte le misure ed i controlli di sicurezza applicati al sistema informativo del Dipartimento per i Trasporti (SIDT) del Ministero con particolare focus sulle misure organizzative e tecnologiche atte a garantire:

- la definizione dei soggetti che, a diverso titolo, possono trattare i dati personali e le funzioni che possono assumere sotto il profilo lavorativo;
- la sicurezza dei dati personali sottoposti al trattamento su tutti gli ambiti applicativi;
- l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi del trattamento.

Le applicazioni del SIDT utilizzano quale infrastruttura di database Oracle DBMS e ciò permette di applicare le misure di sicurezza e le "best practice" direttamente sull'infrastruttura dei dati con il minimo impatto sulle applicazioni.

Criptazione diretta dei dati: grazie alla Transparent Data Encryption (TDE), i dati del database sono cifrati in modo trasparente alle applicazioni, proteggendo le informazioni sensibili contro l'accesso diretto a livello di sistema operativo e dei sistemi di archiviazione (cioè sia i dispositivi di storage che i supporti di backup).

TDE cripta i dati prima di renderli persistenti su disco e trasparentemente li decifra quando vengono acceduti per essere inviati al layer applicativo, dopo che l'utente dell'applicazione, che ne ha fatto richiesta, è stato autenticato e ha superato tutte le verifiche di controllo di accesso sia a livello di applicazione che di database.

TDE fornisce una gestione integrata delle chiavi con architettura a due livelli che prevede una singola chiave master di crittografia memorizzata all'esterno del database e una o più chiavi memorizzate all'interno del database. La chiave master di crittografia è utilizzata per cifrare e proteggere le chiavi memorizzate all'interno del database.

Offuscamento selettivo dei dati sensibili: nel SIDT è possibile anche attivare opzioni di mascheramento dinamico dei dati sensibili nella risposta ad una query, agendo in tempo reale e in modo selettivo. Ciò previene che gli utenti non autorizzati possano visualizzare i dati sensibili. In pratica, si opera dinamicamente sul risultato della query per oscurare, secondo policy stabilite, le informazioni, prima di mostrarle all'applicazione.
Controllo dei privilegi degli accessi degli utenti del database: nel SIDT è attivo anche il controllo dei privilegi limitando il potere degli amministratori del database, prevenendo gli accessi non autorizzati ai dati applicativi e nello stesso tempo lasciando agli amministratori del database i privilegi per le sole attività tecniche.
Integrità, disponibilità, resilienza e ripristino in caso di incidenti: l'intero sistema informativo del Dipartimento per i trasporti adotta tutte le moderne misure atte a garantire l'integrità, la disponibilità e la resilienza dei propri sistemi informatici, nonché la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai medesimi in caso di incidente fisico o tecnico.
Il Dipartimento per i trasporti è datato di un CED primario e di uno secondario (Disaster recovery) che possono erogare i servizi, entrambi con doppia alimentazione elettrica, multipli UPS e Gruppi elettrogeni; doppio impianto di refrigerazione in due diverse tecnologie per il raffrescamento della sala macchine; apparati di rete e di sicurezza in configurazione di alta affidabilità con doppia alimentazione elettrica; server virtuali su infrastruttura hardware virtualizzata; sistemi di archiviazione dati ottimizzati, ecc.
Più specificatamente, per il database ed anche per dati sensibili in esso contenuti, le due database machine "Oracle Exadata", presenti in entrambi i siti primario e secondario, si sincronizzano con flussi dati criptati in tempo reale, portando a zero la perdita di dati in caso di guasto (Recovery Point Objective RPO=0).
Canali di Trasmissione: anche per quanto riguarda i canali di trasmissione utilizzati negli scambi informativi tra i vari soggetti che dovranno accedere agli applicativi erogati dal CED del Dipartimento per i trasporti, si adottano le seguenti misure di sicurezza che portano all'identificazione certa del soggetto che tenta di accedere alla rete del Dipartimento per i trasporti che, in ogni caso, eroga servizi esclusivamente con la criptazione SSL.
Gli uffici della Motorizzazione Civile si collegano al CED del Dipartimento trasporti esclusivamente tramite il Servizio Pubblico di Connettività (SPC), ossia tramite la rete protetta e certificata AgID, gestita direttamente dal MIT a livello di singola postazione di lavoro, nel cosiddetto "ambito Intranet SPC".
Gli Enti pubblici, quali le Forze dell'ordine e gli uffici PRA dell'ACI, si collegano esclusivamente tramite la rete pubblica certificata da SPC, cosiddetto "ambito Infranet SPC", che consente l'identificazione certa della provenienza delle richieste di accesso.
Tutti gli altri soggetti intervengono tramite rete pubblica internet in due modalità: tramite ulteriore rete protetta VPN con accesso al server VPN del Dipartimento per i trasporti, oppure con la necessità di introdurre un ulteriore elemento di autenticazione.

Ministero della salute

MISURE ORGANIZZATIVE
- Il Ministero della salute in qualità di titolare del trattamento di tutti i dati personali trattati nell'ambito delle proprie competenze, attraverso un decreto del proprio Segretario generale, ha individuato nelle figure dei Direttori generali, del direttore dell'ufficio 1 del Segretariato generale, di un dirigente amministrativo dell'ufficio di Gabinetto e di un dirigente amministrativo della struttura tecnica per la misurazione della performance, i soggetti designati per lo svolgimento di funzioni e compiti connessi al trattamento dei dati personali, sotto l'autorità del titolare del trattamento. I soggetti designati al trattamento dei dati personali, nell'ambito della propria sfera di competenza, hanno individuato e nominato, per conto del Titolare, i Responsabili del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, in tutti quei casi in cui, per l'esecuzione di specifiche attività di trattamento ricorrano a soggetti esterni all'Amministrazione. I Designati hanno successivamente individuato i soggetti autorizzati al trattamento dei dati di propria competenza fornendo loro adeguate istruzioni per il corretto trattamento dei dati personali.
- Il Ministero della salute, attraverso specifico decreto del Segretario generale ha provveduto a designare il Responsabile della protezione dei dati (RPD) indicandone i relativi compiti e funzioni, come previsto dall'art. 39 del regolamento (UE) 2016/769, nonché le modalità di interazione con gli altri soggetti (Titolare, responsabili, designati e autorizzati al trattamento).
- Ciascun designato ha contribuito alla realizzazione del registro delle attività di trattamento di cui all'art. 30 del Regolamento (UE) 2016/769, con riferimento agli ambiti di competenza della struttura cui è preposto; ogni soggetto designato è anche responsabile dell'aggiornamento del Registro per la parte di propria competenza. Il Registro è formalmente tenuto presso il Segretariato generale, anche in formato elettronico.
- Sono stati implementati sistemi per la gestione degli accessi ai dati che consentono di individuare diversi profili di accesso per gli utenti autenticati secondo un sistema gerarchico di autenticazione.
- I Responsabili del trattamento sono stati vincolati all'impegno contrattuale di rispettare, nello svolgimento delle attività di propria competenza, le misure tecniche ed organizzative concordate con il Ministero della salute, ritenute idonee per garantire un livello di sicurezza adeguato al rischio connesso allo svolgimento di tali attività. In particolare Il CED ove sono posti i server e le banche dati è certificato secondo la norma ISO/IEC 27001 e gestito da un fornitore qualificato, dotato di un sistema di controllo accesso fisico costituito da un servizio di guardiania 24hx7 gg e bussole di accesso con autenticazione tramite badge.

MISURE TECNICHE
- L'Amministrazione adotta un sistema di controllo degli accessi alle informazioni ed ai sistemi di elaborazione delle informazioni allo scopo di consentire un accesso controllato a tali risorse ai soli utenti autorizzati. Sono state quindi definite politiche, procedure e controlli conformi alla normativa vigente in materia. L'accesso ai sistemi e alle informazioni è consentito ai soli utenti autorizzati e limitatamente ai sistemi e informazioni che essi necessitano di conoscere (principio del need-to-know). I diritti di accesso degli utenti (autorizzazioni, modifiche e rimozione) sono gestiti in accordo ai profili di autorizzazione assegnati. Inoltre sono disponibili degli strumenti per il controllo degli accessi.
- Per la gestione delle utenze sono implementate procedure per la registrazione e la de-registrazione degli utenti, l'assegnazione dei diritti di accesso, l'utilizzo di user ID univoche per consentire il collegamento tra gli utenti e le loro azioni, la verifica periodica dei diritti di accesso degli utenti.
- Il sistema di gestione delle password implementato soddisfa i seguenti requisiti di sicurezza: Obbligo di cambiare la password iniziale al primo accesso, lunghezza minima di 8 caratteri, obbligo di utilizzare nella formazione della password caratteri maiuscoli, minuscoli, numeri e speciali, scadenza 90 giorni, obbligo di utilizzare un certo numero di password diverse prima che si possa impostare una password già utilizzata (Historysize), password codificate e memorizzate in repository dedicati e separati dagli altri dati.

- Per la sicurezza delle postazioni di lavoro sono adottate diverse misure di sicurezza quali il controllo di accesso tramite userid/password, la profilazione degli utenti, l'utilizzo di Antivirus e Antispamming.
- Inoltre, relativamente ai privilegi di amministratore delle postazioni di lavoro questi sono utilizzati solo per la gestione della postazione e sono tracciati conformemente al provvedimento del garante del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
- Ove ritenute necessarie sono adottate tecniche di pseudonimizzazione come la codifica e la Crittografia.
- Le misure di sicurezza adottate per la protezione dei dati sono correlate al loro livello di classificazione conformemente alla normativa sulla protezione dei dati e alle misure minime di sicurezza AGID.
- Le principali misure di sicurezza implementate sono il controllo degli accessi, la profilazione degli utenti, la registrazione delle operazioni, l'utilizzo di Antivirus, il Patching dei sistemi, attività di monitoraggio, l'uso di Firewall perimetrali e tra le diverse reti logiche, l'adozione di sistemi IDS/IPS, la crittografia dei canali di comunicazione. Inoltre, l'adeguatezza di queste misure è verificata periodicamente mediante attività di riskassessment e vulnerabilityassessment.
- Il Ministero dispone di un sistema GAF – Gestione Accoglienza Flussi che consente, in fase di acquisizione dei dati, di effettuare dei controlli formali di coerenza e completezza restituendoli attraverso un'apposita reportistica agli utenti per consentire loro la correzione dei dati. Inoltre sono stati messi a disposizione degli utenti che inviano i dati strumenti di Business intelligence per effettuare confronti e analisi attraverso il calcolo di specifici indicatori individuati in base al tipo di flusso informativo.
- L'Amministrazione, così come il Fornitore di servizi di Informatici, dispongono di procedure per La gestione degli incidenti di sicurezza e la gestione dei data breach .
- Per il ripristino della disponibilità dei dati in caso di incidente fisico o tecnico sono implementate politiche e procedure di backup per tutti i dati, sistemi in alta affidabilità e misure per la continuità operativa e il DisasterRecovery.
- Il CED è dotato di sistemi per la cancellazione sicura dei dati in conformità al Provvedimento "Rifiuti di apparecchiature elettriche ed elettroniche (Raee)" e misure di sicurezza dei dati personali. Per i documenti cartacei sono disponibili dispositivi per lo sminuzzamento dei fogli.
- Le modalità adottate per la trasmissione dei dati prevedono canali sicuri di comunicazione quali ad esempio http su SSL, VPN e FTP sicuro.

Presidenza del consiglio dei ministri

Al fine della piena applicazione del GDPR è stato adottato il DPCM 25 maggio 2018 che disciplina l'organizzazione e la gestione del trattamento dei dati personali all'interno della Presidenza del Consiglio dei ministri (PCM). L'art. 2 del DPCM stabilisce che titolare del trattamento è la PCM nelle sue articolazioni organizzative e all'art. 3 specifica che i soggetti individuati per l'esercizio del trattamento sono: i capi di Dipartimenti, Uffici autonomi, Uffici di diretta collaborazione, i coordinatori delle strutture di missione, della segreteria tecnica Commissione Adozioni internazionali, del Servizio voli di Stato.
Pertanto, sono titolari del trattamento dei dati personali in ambito PSN i Capi delle strutture titolari dei lavori.
Ogni titolare del trattamento: impartisce le istruzioni a tutti i dirigenti coinvolti nel trattamento; definisce finalità e mezzi di trattamento; designa gli autorizzati al trattamento dei dati personali; gestisce il rapporto con il responsabile del trattamento; nomina un Referente privacy.
Lo stesso art. 2 esclude alcune strutture della PCM dall'applicazione del DPCM e individua quali autonomi titolari del trattamento: le strutture dei Commissari straordinari del Governo di cui all'art. 11 della L. 400/88; le strutture dei Commissari straordinari incaricati sulla base di leggi speciali; le strutture dei rappresentanti del Governo nelle Regioni e nelle Province autonome di Trento e di Bolzano; il Dipartimento della protezione civile; la Scuola nazionale dell'Amministrazione; l'Unità tecnico-amministrativa di Napoli. Tali strutture, ai sensi dell'art. 2 co. 5 del medesimo DPCM, designano autonomamente il proprio RPD.
Le misure organizzative e tecniche qui esposte si riferiscono alle strutture coinvolte nel Psn, titolari dei lavori a regime che trattano dati personali, in particolare il Dipartimento per la funzione pubblica (DFP) (per PCM-00030) e la Segreteria tecnica della Commissione Adozioni Internazionali (CAI) (per PCM-00033).

MISURE ORGANIZZATIVE

- *Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento*

per PCM-00030, nomina del Responsabile del trattamento (Fornitore dei servizi di sviluppo) come previsto da Contratto e richiesta a questi di adesione al codice di condotta e ai meccanismi di certificazione previsti;
per PCM-00033, nomina del Responsabile del trattamento esterno (il fornitore di assistenza all'infrastruttura tecnica della Segreteria Tecnica della CAI, per contratto, è il responsabile esterno del trattamento ex art. 28 del GDPR). Con specifici ordini di servizio (OdS) sono stati definiti i ruoli e le responsabilità nei soggetti coinvolti nel trattamento dei dati: referenti della conservazione e archiviazione dei documenti ed approvazione di linee guida in materia di archiviazione cui deve attenersi tutto il personale; referente privacy e istituzione di un gruppo di lavoro privacy; personale autorizzato al trattamento dei dati personali; consegnatario chiavi dei locali in cui sono posti i server dedicati alla conservazione dei dati sulle procedure adottive e relative istruzioni sulle modalità di accesso ai locali CED e tenuta del registro dei relativi accessi; individuazione del responsabile della conservazione dei documenti cartacei ed informatici.

- *Gestione delle autorizzazioni all'accesso ai dati*

per PCM-00030, è previsto che il DFP gestisca il processo di autorizzazione per il ruolo di Responsabile dell'Amministrazione, mentre gli Inseritori degli incarichi sono sottoposti a processo di autorizzazione da parte del proprio Responsabile;
per PCM-00033, i dati trattati dalla CAI risiedono nel sistema informatico gestionale denominato "SVEVA", composto dei seguenti moduli operativi: " SVEVA Workflow" (per operare sui dati, secondo i diversi ruoli assegnati, in intranet con autenticazione di dominio caiwork.pcm.it); "SVEVA Gestionale Enti" (per l'accesso degli Enti autorizzati su internet con autenticazione tramite "username", "password", data di scadenza dell'accesso determinata da "chiave pubblica" del certificato digitale, con un ulteriore controllo denominato "utente attivo"); "Adozione Trasparente" (portale su Internet riservato esclusivamente ai cittadini che hanno un fascicolo adottivo su SVEVA, il cui accesso avviene unicamente tramite autenticazione SPID). Ai moduli indicati si aggiunge lo strumento di share di rete condivisa il cui accesso è determinato tramite utenza di dominio caiwork.pcm.it ed i cui diritti sono connessi ad ambiti di competenze lavorative.

- *Interventi posti in essere per la formazione del personale*

per PCM-00030, sono stati previsti video introduttivi formativi;

per PCM-00033,sono stati effettuati corsi di formazione per il titolare ed il referente privacy e sono stati richiesti corsi per tutto il personale della Segreteria Tecnica.

- *Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici*

per PCM-00030, predisposto il Registro del titolare del Trattamento viene aggiornato in caso di variazione delle condizioni;
per PCM-00033, l'accesso delle persone nel CED della CAI viene registrato su apposito "registro degli accessi al CED", di norma viene consentito solo a figure tecnico/informatiche per attività di controllo su apparecchiature e locali. L'eventuale accesso a personale estraneo alla CAI viene sempre registrato sul registro e comunque è soggetto al Pass di controllo accessi della sede CAI.

- *Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi*

per PCM-00030, Banca dati in CLOUD. Accessi gestiti secondo politica dal fornitore dei relativi servizi (certificato ISO 27001) e secondo quanto stabilito dalla convenzione SPC-CLOUD Lotto1;

- *Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati") e adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati:*

per PCM-00030, la Policy privacy è pubblicata sul sito;
per PCM-00033, le informative ex art. 13 e 14 sono a disposizione in formato PDF sul portale CAI Adozione Trasparente. L'accesso alla piattaforma gestionale SVEVA permette alla coppia adottiva di prendere visione del loro fascicolo personale. Sul sito è disponibile la privacy policy dello stesso.

- *Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei*

per PCM-00033,è previsto dal citato Regolamento (DPR 108/07) anche il trattamento cartaceo in relazione alle competenze istituzionali della CAI. In particolare, la Segreteria Tecnica (ST) ha emesso ordini di servizio che prevedono linee guida per le modalità di archiviazione e la conservazione dei supporti cartacei. È inoltre predisposto un rapporto annuale sulla gestione dell'archivio cartaceo ed è elaborato semestralmente un rapporto sul trasferimento negli archivi della PCM dei dossier adottivi chiusi allo scopo di mantenere presso la ST solo l'archivio corrente.

- *Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati*

per PCM-00033, è previsto dal citato Regolamento (art. 7 co. 5 del DPR 108/07) che la CAI può effettuare il trattamento dei dati particolari relativi al minore, alla sua famiglia di origine, ai genitori adottivi in forma anonima limitatamente per i dati indispensabili allo svolgimento delle singole procedure di adozione; la diffusione dei dati può essere effettuata solo in forma anonima e per finalità statistiche, di studio, di informazione e ricerca.

MISURE TECNICHE

- *Sistema di autenticazione individuale degli utenti e tracciamento degli accessi*

per PCM-000030, accesso tramite sistema di autenticazione individuale;
per PCM-00033, autenticazione individuale di dominio e log sia di sistema che dell'applicativo SVEVA per il tracciamento delle operazioni;

- *Adozione di sistemi perimetrali di controllo*

per PCM-000030, Firewall e IDS/IPS sulla rete perimetrale dell'infrastruttura e Virtual firewall come servizio IaaS;
per PCM-000033, ai locali della Segreteria Tecnica della Commissione per le adozioni internazionali si accede solo su invito e previa registrazione dell'accesso.

- *Adozione di misure per garantire la qualità e la correttezza dei dati*

per PCM-000030, ciascun utente può modificare i soli dati di cui è responsabile;
per PCM-000033, i genitori adottivi accedono, tramite SPID, al loro fascicolo personale attraverso la piattaforma "Adozione Trasparente" che permette alla coppia adottiva di monitorare il proprio dossier e di verificare la qualità e la correttezza del dato presente in archivio digitale e di interagire con la CAI in merito.

- *Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679*

per PCM-00030, Sistema di Monitoraggio dei servizi presenti sulla componente IaaS di SPC-Cloud;
- Eventuali problemi tecnici sono monitorati attraverso il servizio di monitoraggio della piattaforma.
- Segnalazione e gestione:

a) "Procedura per l'esercizio e notifica della violazione dei diritti dell'interessato" (ex artt. 15-22 del GDPR)
b) "Procedura di gestione del databreach" (ex artt. 33 e 34 del GDPR) e la Notifica della violazione dei dati all'Autorità di Controllo (Garante della Privacy) [pubblicate sul "Portale di Governo e gestione della fornitura"].
c) "Procedura per la gestione degli incidenti di sicurezza";

per PCM-00033, adozione di un registro di data breach.

- *Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)*

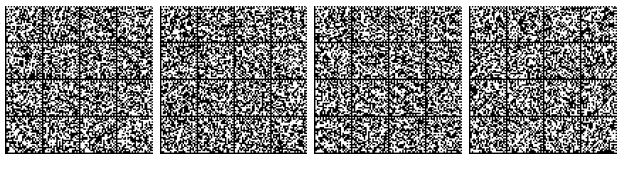
per PCM-00030, il backup dei dati dei clienti è effettuato nell'ambito del servizio BaaSManaged ed è presente un servizio di Internal backup per l'infrastruttura SPC Cloud;
per PCM-00033, vengono effettuati backup giornalieri e settimanali, sia totali che incrementali dei dati, ridondati su più dispositivi.

- *Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche*

per PCM-00030, la distruzione dei supporti magnetici è effettuata tramite un servizio esterno da ditta specializzata (degausser o triturazione meccanica) con videoregistrazione delle operazioni di cancellazione;

- *Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni*

per PCM-00030, per la trasmissione sulle reti pubbliche è utilizzato il protocollo HTTPS;
per PCM-00033, le comunicazioni con gli Enti Autorizzati ad esecuzione delle procedure adottive avvengono tramite la piattaforma SVEVA che garantisce l'integrità, la disponibilità e la riservatezza delle informazioni.



Provincia autonoma di Bolzano

MISURE ORGANIZZATIVE

Pur svolgendo la propria attività in forte autonomia, l'Istituto è inserito nell'Amministrazione provinciale e pertanto si avvale di alcune tipologie di servizi resi in forma centralizzata. La Provincia autonoma ha nominato il Responsabile per la protezione dei dati personali e gestisce l'archivio complessivo dei trattamenti per l'Amministrazione provinciale.

L'ASTAT ha un proprio archivio dei trattamenti collegato ad un archivio degli incaricati ai trattamenti. Nell'archivio dei trattamenti sono elencate le banche dati gestite dall'ASTAT, con informazioni sulle variabili, sulle modalità di trattamento e sulle persone coinvolte nel trattamento.

Responsabile dei trattamenti è il Direttore pro tempore dell'ASTAT, che procede alla nomina degli incaricati.

Ogni incaricato ai trattamenti prende visione e sottoscrive, al momento dell'assunzione e successivamente con periodicità almeno annuale, il documento di nomina, in cui sono elencati i tipi di dati e le modalità del trattamento, nonché i principali obblighi di comportamento. Presso la segreteria dell'ASTAT sono raccolti tutti i documenti di nomina degli incaricati al trattamento. Nel documento di nomina è descritto il grado di accesso ai dati e le caratteristiche essenziali del trattamento.

In caso di trattamento dei dati svolto da soggetti esterni per conto dell'ASTAT, nel documento di incarico viene formalizzata la designazione di un responsabile del trattamento, con descrizione delle disposizioni e delle istruzioni da seguire nel trattamento.

Tutto il personale dell'ASTAT riceve all'atto dell'assunzione un'adeguata formazione sulla normativa inerente la tutela dei dati personali. In occasione di modifiche normative, ma comunque con periodicità almeno biennale, vengono effettuati workshop illustrativi.

Il personale dell'ASTAT partecipa con regolarità ai corsi di aggiornamento sulle disposizioni inerenti le Regole deontologiche e di comportamento nei trattamenti a scopi statistici, nonché riguardo alle normative relative al segreto statistico ed al Codice delle statistiche europee. I dipendenti dell'ASTAT sono altresì tenuti al rispetto delle disposizioni previste nel Codice di comportamento della Provincia autonoma di Bolzano.

L'accesso fisico ai locali dell'ASTAT è regolato attraverso l'utilizzo di badge personali con foto e firma per tutti i dipendenti. L'ingresso è sorvegliato da personale incaricato, che provvede ad accompagnare eventuali visitatori o consulenti esterni. L'accesso alle aree riservate e alle stanze tecniche è autorizzato al solo personale formalmente incaricato, previa richiesta scritta. All'ingresso dell'edificio è presente un sistema di videocamere di sorveglianza.

In caso di indagini dirette, che prevedono l'acquisizione dei dati direttamente presso gli interessati, viene loro recapitata una lettera informativa del Direttore dell'ASTAT, nella quale sono descritte sia le finalità del trattamento, sia le modalità in cui questo avviene, sia la possibilità che i dati rilevati possano essere utilizzati anche per ulteriori trattamenti statistici, nonché l'obbligatorietà o meno del conferimento dei dati. Nei casi in cui i dati siano rilevati presso soggetti terzi e non sia agevole contattare gli interessati, l'informativa a questi ultimi viene resa attraverso il Programma statistico.

MISURE TECNICHE

L'accesso alle infrastrutture tecnologiche dell'ASTAT prevede l'utilizzo di credenziali individuali fornite ad ogni dipendente al momento dell'assunzione, con rinnovo periodico obbligatorio. Ogni accesso viene tracciato e conservato per un periodo minimo di tre mesi.

Sono adottate misure per garantire la sicurezza informatica della postazione di lavoro, con l'utilizzo di sistemi di sicurezza firewall e antimalware ad aggiornamento automatico continuo. Come tutta l'Amministrazione provinciale, anche l'ASTAT è seguita dal partner informatico SIAG (Informatica Alto Adige-Südtiroler Informatik AG, società in house della Provincia autonoma di Bolzano) che si occupa di tenere aggiornati i sistemi informativi utilizzati da ASTAT.

I dati personali provenienti da fonti amministrative vengono sottoposti a procedure di pseudonimizzazione, con separazione dei codici identificativi diretti degli interessati dalle altre informazioni personali. La tabella di raccordo tra gli identificativi diretti e i codici pseudonimizzati è conservata separatamente ed utilizzata solo al fine di aggiornare il raccordo tra questi.

Il sistema informativo usufruisce di un datacenter di disaster-recovery per garantire il ripristino in seguito ad eventi catastrofici sui datacenter primari. I dati sono archiviati su supporti durevoli attraverso appositi sistemi di backup.

I dati riguardanti l'appartenenza linguistica delle persone verranno trattati con modalità che non consentiranno agli incaricati del trattamento di ricondurre il dato alla persona interessata. È ancora in fase di progettazione il dettaglio delle modalità di raccolta e successiva elaborazione dei dati. I dati verranno distrutti successivamente alla loro diffusione in forma aggregata.

Provincia autonoma di Trento

MISURE ORGANIZZATIVE

La sede dell'ISPAT si trova al quinto e sesto piano di una struttura provinciale in via Zambra n. 42 a Trento: l'accesso agli uffici, alle sale riunioni, ai laboratori ADELE e LAD è controllato da personale di portineria e per accedere alla struttura occorre munirsi di appuntamento e firmare un registro presenze in caso di accesso ai laboratori. La documentazione cartacea con eventuali dati personali/sensibili è adeguatamente protetta in armadi chiusi a chiave con accessi limitati a personale determinato. La stragrande maggioranza degli archivi sono in forma digitale sia per una massiccia dematerializzazione promossa dalla Provincia autonoma di Trento, sia per la comodità di utilizzo e di protezione dei dati trattati.

La struttura mantiene aggiornato con cadenza periodica il *Registro elettronico dei trattamenti dei dati* e procede all'adempimento di quanto richiesto dalla normativa: designa i soggetti che sono autorizzati al trattamento dei dati, inserisce il trattamento nel registro prima che lo stesso venga eseguito, designa Responsabili esterni quando è necessario, promuove la cultura della protezione dei dati in occasione di nuovi trattamenti (c.d. *privacy by design*), cura l'aggiornamento continuo e la formazione del personale, anche con riferimento al segreto statistico oltre che alla protezione dei dati personali.

Tutti i trattamenti prevedono il conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati") e nei termini previsti dal Registro si procede alla cancellazione dei dati non più necessari all'Istituto.

MISURE TECNICHE

I dati personali oggetto di trattamento sono custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'accesso agli archivi informatizzati è regolato attraverso autenticazione informatica e tracciamento degli accessi; le credenziali di accesso sono obbligatoriamente modificate ogni 60 giorni. Ogni incaricato del trattamento ha accesso ai soli archivi per i quali è stato autorizzato;

l'accesso agli archivi è regolato attraverso la gestione delle *permission*. Di ogni archivio informatizzato esistono copie di sicurezza conservate in luogo idoneo e diverso da quello in cui sono conservati i dati originali, con accesso riservato e/o in armadi chiusi a chiave.
La sicurezza dei *server* sui quali sono memorizzati i dati originali e le copie (*backup*) è garantita dalla società di sistema della Provincia autonoma di Trento (Trentino Digitale S.p.A.), incaricata di svolgere la funzione di Amministratore di sistema e designata quale Responsabile esterno dei trattamenti dei dati per l'intera Provincia autonoma di Trento.
Gli incaricati del trattamento sono designati per iscritto e come già specificato tutti i trattamenti sono gestiti nel *Registro elettronico dei trattamenti dei dati.*
La designazione individua l'ambito del trattamento consentito e impartisce le istruzioni per la protezione dei dati personali. Agli incaricati del trattamento sono impartite istruzioni per non lasciare incustodita e accessibile la postazione elettronica durante la sessione di trattamento.
I dati identificativi sono conservati separatamente da ogni altro dato elementare per il tempo necessario alla validazione del dato statistico (attività di controllo, qualità e copertura). Nel caso delle indagini longitudinali i dati elementari sono pseudonimizzati e gli identificativi sono conservati separatamente da ogni altro dato.
I dati elementari vengono conservati per il tempo strettamente necessario alla validazione della rilevazione e alla predisposizione delle elaborazioni statistiche e successivamente vengono eliminati. Comunque non vengono conservati oltre i 24 mesi.

Regione Campania

MISURE ORGANIZZATIVE

Con Deliberazione della Giunta Regionale della Campania n. 466 del 17/08/2018 sono state approvate le prime misure di adeguamento al Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 - General Data Protection Regulation (GDPR). Con tale provvedimento sono state impartite a tutte le Strutture dell'Amministrazione regionale istruzioni e misure relative alla protezione dei dati personali.
In particolare, viene delineato, nell'ambito dell'organizzazione regionale, l'Organigramma privacy, così composto:
- Titolare del trattamento
Il "Titolare del trattamento" dei dati personali effettuati dalle Strutture organizzative della Giunta Regionale della Campania, in continuità con quanto previsto in vigenza delle normative precedenti, è la Giunta Regionale;
- Delegati al trattamento
Delegati al trattamento sono tutti i Dirigenti in servizio presso la Giunta regionale, sia a tempo determinato che a tempo indeterminato, di ruolo o incaricati di incarico dirigenziale ai sensi della vigente normativa, ognuno per la parte di competenza relativa al trattamento dei dati personali effettuato nello svolgimento dell'incarico ricevuto, secondo le previsioni del rispettivo contratto individuale di lavoro;
- Referenti privacy
Ogni Ufficio di livello dirigenziale dovrà nominare un proprio "Referente privacy", che dovrà coadiuvare il Dirigente nell'espletamento dei molteplici compiti afferenti la tematica del trattamento dei dati personali svolti dall'Ufficio.
- Responsabili esterni del trattamento
I Responsabili esterni sono tutti quei soggetti che, essendo "esterni" all'Amministrazione regionale (quali ad esempio società, consulenti, collaboratori, altri enti ecc.) trattano dati personali per conto dell'Amministrazione regionale.
Come espressamente previsto dall'articolo 28 del Regolamento 2016/679/UE, la legittimazione al trattamento di dati personali di cui è titolare la Giunta Regionale della Campania da parte di detti soggetti deve avvenire a seguito di stipula di apposito contratto, con le previsioni dettate dal citato articolo 28 nonché gli obblighi di cui agli articoli 30 e 33 del medesimo Regolamento.
- Sub-responsabili esterni del trattamento
I Responsabili esterni del trattamento possono, se previamente autorizzati per iscritto e con idonea formalizzazione, affidare alcuni trattamenti di dati personali a sub-responsabili esterni.
- Persone autorizzate al trattamento
Si tratta di tutti quei soggetti che, all'interno di una Struttura dirigenziale e per le materie di competenza, effettuano trattamenti di dati personali nell'espletamento dei propri compiti istituzionali. Il Regolamento prevede che tali trattamenti avvengano sotto l'autorità diretta del Titolare o del Responsabile, i quali garantiscono che gli stessi si siano impegnati alla riservatezza o posseggano un adeguato obbligo legale di riservatezza.
- Responsabile della protezione dei dati personali
Con Decreto del Presidente della Giunta Regionale della Campania n. 78 del 25/05/2018 è stato nominato il DPO nella persona del dott. Eduardo Ascione, Dirigente dell'Ufficio III della Segreteria di Giunta.
- Gestione delle autorizzazioni all'accesso ai dati.
In forza del citato organigramma, pertanto, sono attribuiti a ciascun Dirigente regionale i compiti e le funzioni connessi al trattamento dei dati personali afferenti agli ambiti di rispettiva competenza. Ad essi compete, altresì, il compito di fornire specifiche istruzioni ai propri collaboratori sulle modalità di trattamento dei dati e sulle misure da adottare per garantire la protezione dei dati personali, la verifica periodica della sussistenza delle condizioni per il mantenimento delle autorizzazioni al trattamento e, nel caso esse non sussistano, la revoca delle stesse.
Gli Uffici regionali hanno provveduto ad incaricare formalmente al trattamento dei dati il personale ivi in servizio con disposizioni scritte. Anche l'individuazione dei responsabili esterni ex articolo 28 del Regolamento e i trattamenti a essi affidati sono disciplinati in appositi atti scritti.
- Interventi posti in essere per la formazione del personale
Nel corso dell'anno 2019 è stato pianificato un percorso formativo denominato "la privacy: profili teorici ed aspetti pratici". Esso è stato erogato, in modalità d'aula, ai Dirigenti delegati dal Titolare e ai Referenti Privacy delle Strutture ed, in modalità webinar, ai funzionari ed agli istruttori della Giunta Regionale della Campania.
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679 (G.D.P.R.)
Ai sensi dell'articolo 30 del Regolamento è stato istituito il *Registro dei trattamenti di dati personali*. Nel registro sono descritte, per ciascun trattamento, la finalità, la tipologia dei dati (personali e/o non personali, rientranti nelle particolari categorie di cui all'articolo 9 del G.D.P.R., i dati relativi a condanne penali e reati, di cui all'articolo 10 del medesimo Regolamento), le strutture interne e/o esterne che effettuano o concorrono al trattamento, le caratteristiche delle banche dati utilizzate con la loro ubicazione fisica e gli estremi degli atti di autorizzazione al trattamento dei dati personali.

Il registro è oggetto di monitoraggio continuo ai fini del suo aggiornamento/integrazione al mutare dei trattamenti di competenza dei singoli Uffici regionali.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

L'accesso fisico agli Uffici avviene con l'utilizzo di badge personali con foto. Esiste un sistema di videosorveglianza e guardie giurate h. 24. Per i visitatori è previsto l'accesso previa consegna di un documento di riconoscimento e contatto con l'ufficio di destinazione del visitatore. L'accesso alle aree "sala CRED" è autorizzato al solo personale formalmente incaricato. Alle sale si accede con codici di accesso. I singoli PC sono protetti da Password che vanno modificate periodicamente pena sospensione degli accessi. Le porte d'accesso sono provviste di chiavi.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

Per l'esercizio dei propri diritti ciascun interessato può contattare il responsabile della protezione dei dati della Regione Campania.

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei

Per i trattamenti che prevedono il supporto cartaceo, gli stessi vengono manipolati dal solo personale autorizzato e riposti in armadi chiusi a chiave.

MISURE TECNICHE

La sicurezza dei dati, dei sistemi e delle infrastrutture è garantita da:
- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di sistemi perimetrali di controllo;
- Utilizzo di tecniche di cifratura e/o pseudonimizzazione;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Modalità di cancellazione sicura dei dati in caso di dismissione di apparecchiature elettroniche;
- All'interno dell'Ufficio di statistica i dati risiedono su pc il cui accesso è consentito solo al personale autorizzato e munito di password;
- I dati elementari personali vengono trasmessi all'esterno solo a enti SISTAN utilizzando sistemi sicuri di trasmissione messi a disposizione dall'Istat.

Regione Emilia Romagna

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)

Con la deliberazione n. 1123/20183 la Giunta regionale ha attribuito in capo al Capo di Gabinetto, ai Direttori generali, al Direttore dell'Agenzia Sanitaria e sociale regionale, al Direttore dell'Agenzia informazione e comunicazione, al dirigente competente in materia statistica precipue funzioni e responsabilità in materia di protezione dei dati personali. Con tale atto è stata operata una netta separazione delle aree di responsabilità previste in capo ai dirigenti delle strutture, funzionale alla riduzione di opportunità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione.

La sicurezza informatica, comprensiva del coordinamento sull'applicazione della normativa sulla protezione dei dati personali, è competenza del Servizio ICT Regionale che svolge l'attività anche quale strumento del Responsabile per la Transizione Digitale. A tale struttura, tra le altre cose, competono i contatti con le Autorità7 (come ad es. con la Polizia postale e CSIRT) e con i gruppi specialistici8 (ad. Es. CLUSIT). Sono state disciplinate le interazioni di tali figure con il DPO nominato.

- Gestione delle autorizzazioni all'accesso ai dati

Dipendenti e collaboratori, ai sensi dell'art. 2quaterdecies del d.lgs. 196/2003 sono autorizzati con determinazione dirigenziale, come prescritto nel modello organizzativo sopra citato.

- Interventi posti in essere per la formazione del personale

È stato di recente somministrato a tutti i dipendenti/collaboratori regionali un corso sul GDPR e sulle modalità di attuazione della normativa nell'Ente. Ogni anno viene redatto un piano della formazione del personale che viene aggiornato periodicamente con le nuove esigenze formative e viene pubblicato sulla intranet regionale.

- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici

L'Ente ha adottato un registro dei trattamenti sin dal 2005. In questi anni il registro è stato perfezionato e arricchito di informazioni e registrazioni. È stato progettato un nuovo registro, dinamico e relazionato con altre piattaforme regionali, che andrà in produzione entro la fine del 2020.

- Modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto

In caso di trattamento dei dati svolto da soggetti esterni, gli stessi sono nominati responsabili del trattamento a mezzo di uno strutturato accordo allegato al contratto. La struttura competente in materia di privacy ha prodotto e condiviso nella intranet un fac-simile cui tutte le strutture dell'ente si conformano. La nomina dei responsabili del trattamento è uno dei compiti che la Giunta ha attribuito ai Direttori generali nel modello organizzativo sopra citato.

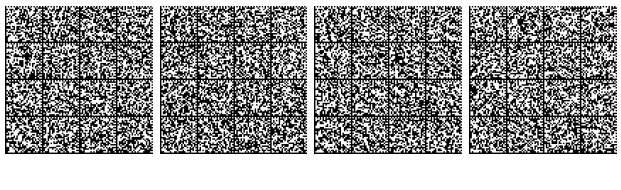
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

Il disciplinare tecnico regionale, approvato con la determina 1894 del 14/02/2018 ha regolamentato l'accesso alle sedi dell'Ente al fine di ridurre i rischi derivanti dall'accesso di soggetti non autorizzati alle sedi dell'Ente. Per ragioni di sicurezza, data la rilevante natura strategica e operativa del Datacenter, i locali che lo ospitano sono limitati da porte la cui apertura richiede l'utilizzo di uno specifico badge. Tali badge sono rilasciati solo previa autorizzazione. Sono attivi sistemi di allarmi e videosorveglianza. Gli accessi al datacenter sono presidiati da portineria e vigilanza.

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Nel rispetto delle disposizioni normative in materia di trattamento dei dati personali, i soggetti interessati sono informati del trattamento dei dati attraverso apposite informative. Per le fonti di dati raccolti presso soggetti terzi, l'informativa, anche per i trattamenti con finalità statistiche, è resa all'interessato al momento dell'acquisizione del dato. L'informativa è altresì resa attraverso il Programma Statistico Nazionale in cui sono descritte le caratteristiche dei trattamenti statistici effettuati.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati



L'Ente ha adottato con la Determina n. 14128 del 30/07/2019 un Disciplinare per l'esercizio dei diritti dell'interessato sui propri dati personali (Giunta e Assemblea), per disciplinare il workflow e le responsabilità al fine di adempiere agli oneri derivanti dalla normativa.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

L'Ente ha implementato e formalizzato un articolato processo di provisioning per l'assegnazione o la revoca dei diritti di accesso, per le diverse tipologie di utenze e per i diversi sistemi e servizi. L'assegnazione di informazioni segrete di autenticazione è controllata attraverso un processo di gestione formale sia per utenti ordinari che per amministratori di sistema.

I diritti di accesso di tutto il personale, ivi compresi i collaboratori a qualsiasi titolo, sono riesaminati a mezzo delle verifiche di sicurezza che sono effettuate a campione sulle strutture dell'Ente, oltre che su specifica segnalazione. Gli account sono, pertanto, rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, e, in ogni caso, in relazione alle modifiche intervenute nel rapporto di lavoro con l'Ente.

È implementata l'autenticazione di dominio e una soluzione di Privileged Account Management. Le policy di gestione delle password sono le seguenti: lunghezza minima: 10 caratteri; scadenza: 90 giorni; blocco amministrativo: 180 giorni dal primo giorno di non utilizzo; cambio al primo login: attivo.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

Le configurazioni delle postazioni di lavoro del personale dell'Ente sono gestite in maniera centralizzata. La funzione Q0000453 è titolata responsabile di autorizzare l'installazione esclusiva dei software sulle stazioni di lavoro attraverso strumenti automatici e/o interventi da parte dei referenti informatici. In accordo alle politiche di gestione delle postazioni di lavoro, ciascun utente è tenuto a mantenere sulla propria postazione di lavoro la configurazione standard dei programmi di base e dei programmi applicativi installati e non deve interferire, impedire o ritardare la distribuzione centralizzata degli aggiornamenti del software della postazione stessa.

- Utilizzo di tecniche di pseudonimizzazione

I dati personali provenienti da fonti amministrative vengono sottoposti a procedure di pseudonimizzazione nella fase successiva all'acquisizione del dato e comunque prima dell'integrazione dei diversi registri, che avviene attraverso chiavi non identificative anche al fine della minimizzazione dei dati.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

In fase di integrazione di fonti con presenza di dati di particolare natura il trattamento statistico avviene con soluzioni procedurali specifiche definite nelle singole schede del Piano Statistico Nazionale.

- Adozione di misure per garantire la qualità e la correttezza dei dati

I lavori statistici seguono alcuni standard di qualità, come l'utilizzo di classificazioni e definizioni ufficiali o il ricorso a soluzioni metodologiche condivise per il record linkage.

Inoltre, è disponibile per gli incaricati al trattamento la documentazione tecnica al fine di garantire la qualità e la correttezza dei dati durante la fase della raccolta e i successivi trattamenti. La maggior parte di tali misure sono disponibili su web.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

L'Ente ha adottato il Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach (Determinazione n. 212807/2018) e la procedura per la gestione degli incidenti di sicurezza e data breach (con documento registrato nel protocollo regionale).

Tali documenti mirano alla corretta gestione degli incidenti di sicurezza che è misura che consente di evitare o di minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, la corretta attuazione di tale policy e procedura consente di migliorare continuamente la capacità di risposta agli incidenti.

Sono inoltre definite le modalità di registrazione e mantenimento dei log di audit relativi agli accessi e alle attività eseguite dagli utenti sui sistemi e agli eventi di sicurezza. In particolare, la piattaforma di Log Management in uso garantisce il mantenimento dei requisiti di riservatezza, integrità e disponibilità degli eventi di log.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

Il Servizio ICT ha definito una procedura (Procedura di Restore) per il ripristino dei dati. Il Servizio ICT regionale ha definito un Piano di Business continuity per garantire la continuità dei servizi IT a fronte di uno scenario di disastro. L'Ente verifica a intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse. Sono implementati meccanismi di ridondanza su tutte le strutture elaborative che contribuiscono a erogare servizi critici, secondo quanto rilevato attraverso la "Business Impact Analisys (BIA)".

- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche

Al momento della dismissione i dati presenti sugli strumenti elettronici sono cancellati in maniera sicura o attraverso formattazione a basso livello, wiping, smagnetizzazione o distruzione fisica prima del loro riutilizzo e della loro dismissione, come indicato esplicitamente nella policy dedicata agli Amministratori.

- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni

Con particolare riferimento ai dati riservati dell'Ente (ad es. ex sensibili, di autenticazione, identificativi della sessione utente ecc.) che transitano su reti pubbliche sono implementati meccanismi di protezione a mezzo del protocollo di crittografia TLS 1.1 .

Si specifica che le applicazioni informatiche impiegate per il trattamento dei dati personali di natura particolare (precedentemente sensibile) e/o relativi a reati (precedentemente giudiziaria), sono state applicate diverse misure tecniche per garantire la non associabilità diretta del dato all'interessato:

a) meccanismi di cifratura delle comunicazioni: trasmissione dei dati su canali cifrati (es. HTTPS, SFTP, SSH, Host-on-demand over SSL, ecc.);

b) separazione logica dei dati identificativi da quelli sensibili e/o giudiziari: archiviazione in tabelle diverse dei dati identificativi e di quelli sensibili e/o giudiziari, impiegando chiavi esterne per consentire la relazione fra i dati tramite procedure autenticate ed autorizzate (es. visualizzazione di entrambe le tipologie di dati al personale autorizzato all'accesso);

c) meccanismi di cifratura delle comunicazioni verso i Database Oracle.

Regione Lazio

Misure adottate in riferimento al lavoro "*Studio longitudinale della Regione Lazio: disuguaglianza di salute determinate da differenze socio-economiche*" (cod. LAZ-00006)

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati);
- Gestione delle autorizzazioni all'accesso ai dati;
- Interventi posti in essere per la formazione del personale;
- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto.

MISURE TECNICHE
- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di sistemi perimetrali di controllo;
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno del ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni;
- Utilizzo di tecniche di pseudonimizzazione, nello specifico la procedura è applicata prima dell'integrazione dei diversi registri, che avviene attraverso chiavi non identificative. I dati personali non potranno più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, le quali non sono trattate e sono conservate separatamente.

Regione Marche

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)

Al Comitato di direzione di cui all'art. 8 della L.R. 20/2001, composto dal segretario generale e dai dirigenti di servizio, viene attribuito un *ruolo guida* per l'attuazione del GDPR ed in particolare quello di promuovere adeguate misure organizzative e tecniche al fine di garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla normativa.

Per l'attuazione delle misure sono direttamente coinvolti tutti i dirigenti delle strutture organizzative della Giunta regionale, nella loro veste di delegati al trattamento dei dati personali, per quanto strettamente necessario all'esercizio delle competenze agli stessi assegnate. A tale scopo, i dirigenti potranno avvalersi di una *rete di referenti privacy,* dipendenti deputati nelle diverse strutture organizzative a seguire la tematica del trattamento dei dati personali.

I dirigenti della Giunta regionale, in coerenza con le responsabilità attribuite dalla legge regionale 15 ottobre 2001, n. 20, sono delegati al trattamento dei dati personali necessario all'esercizio delle competenze agli stessi assegnate e sono chiamati a definire ed attuare, secondo le indicazioni del Comitato di direzione, misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea. Nel dettaglio si riporta quanto previsto all'art.4 dell'Allegato alla DGR 1504/18

Art. 4 Delegati del titolare del trattamento

1.I dirigenti delle strutture della Giunta regionale, in qualità di delegati, effettuano i trattamenti necessari all'esercizio delle competenze agli stessi assegnate, nel rispetto dei principi di cui all'art. 5 del RGDP e delle condizioni di liceità di cui all'art. 6 del RGDP. Con riferimento al paragrafo l, lettere c) ed e) dell'art. 6 del RGDP *("il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento"* e *"il trattamento è necessario per l'esecuzione di un compito di interesse pubblico* o *connesso al! 'esercizio di pubblici poteri di cui è investito il titolare del trattamento")* il comma l dell'art. *2-ter* del Codice Privacy specifica che la base giuridica è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento; tale specifica dovrà essere riportata nel Registro dei trattamenti di cui all'articolo 8. Il Codice Privacy fornisce all'art. *2-sexies* una elencazione di trattamenti effettuati per motivi di interesse pubblico rilevante.

2. I dirigenti delle strutture della Giunta regionale mettono in atto misure tecniche ed organizzative per garantire il rispetto del Regolamento europeo n. 2016/679 e del Codice Privacy e tengono traccia del percorso logico e delle motivazioni concernenti le scelte effettuate per la tutela della privacy, in attuazione del principio di responsabilizzazione, di cui al paragrafo 2 dell'art. 5 del RGPD. In particolare provvedono a:

a. verificare che il trattamento sia connesso con l'esercizio delle funzioni istituzionali e in generale legittimo; se del caso, provvedono a disporre la cessazione di ogni trattamento che non risponda alle condizioni di liceità di cui all'art. 6 del RGPD;

b. assicurarsi che vengano adottate tutte le misure necessarie a garantire la sicurezza, la qualità, la disponibilità e la conservazione dei dati personali trattati, secondo quanto specificato nel successivo art. 7;

c. aggiornare il registro informatico dei trattamenti di cui all'art. 30 del RGDP, secondo quanto specificato nel successivo art. 8, prima di iniziare il trattamento;

d. individuare formalmente eventuali persone a cui sono attribuiti specifici compiti ai sensi dell'art. 2 *quattordecies* del Codice Privacy, fornendo loro le opportune istruzioni sulle modalità di trattamento ai sensi dell'art. 29 del RGDP e vigilarne l'osservanza;

e. nominare, ove necessario, un responsabile esterno del trattamento ai sensi dell'art. 28 del RGPD e fornire allo stesso le istruzioni ai sensi dell'art. 29 del RGDP;

f. vigilare sull'operato dell'eventuale responsabile esterno;

g. fornire l'informativa di cui agli articoli 13 e 14 del RGPD;

h. predisporre gli strumenti organizzativi al fine di garantire i diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD;

i. procedere alla valutazione dell'impatto sulla protezione dei dati (DPIA), ai sensi dell'art. 35 del RGPD, consultandosi con il Responsabile per la Protezione dei Dati (RPD) ed i responsabili della sicurezza fisica ed informatica. Nel caso in cui la decisione assunta dal dirigente al termine della valutazione sia difforme dalle indicazioni del RPD e/o responsabili sicurezza fisica ed informatica, è necessario motivare specificamente per iscritto tale decisione;

j. collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei propri compiti;
k. informare il Garante della protezione dei dati personali e il RPD, senza ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach");
l. curare l'attuazione dei provvedimenti eventualmente imposti dal Garante.

I dirigenti sono tenuti ad individuare i nominativi dei dipendenti e di eventuali stagisti o collaboratori a vario titolo, che trattano i dati, fornire loro le norme di comportamento e le istruzioni operative necessarie per garantire la conformità al Regolamento UE e vigilare sull'osservanza, secondo un modulo tipo. Il nominativo dei soggetti autorizzati dal dirigente al trattamento dei dati e gli estremi dell'atto con cui sono fornite le istruzioni devono essere riportati nel Registro dei trattamenti. In caso di modifica dei soggetti che trattano i dati, viene aggiornata l'autorizzazione al trattamento con il modello sopra citato, i profili autorizzativi dei sistemi informativi utilizzati per il trattamento e le informazioni sul Registro dei trattamenti. Per i trattamenti effettuati in modalità elettronica la P.F. Informatica e Crescita digitale individua e rivede periodicamente gli elenchi degli Amministratori Di Sistema (ADS) e le figure analoghe nel rispetto del Provvedimento del Garante della Privacy 27.11. 2008 - (G.U. n. 300 del 24 dicembre 2008), relativamente ai sistemi gestiti dalla struttura. Ciascun dirigente provvede alla eventuale nomina ad ADS dei propri dipendenti che svolgano tali funzioni e alle ulteriori incombenze previste dal provvedimento Garante Privacy 27/11/2008, valutando, con il supporto della P.F. Informatica, i requisiti di esperienza, capacità e affidabilità del soggetto designato
Di tutte le questioni concernenti la protezione dei dati ciascun dirigente informa tempestivamente ed adeguatamente il RPD. In relazione all'attività di consulenza, lo staff del RPD attraverso la casella RPD@regione.marche.it assicura una costante attività di supporto alle strutture. Per situazioni di particolare complessità o delicatezza, per le quali si renda opportuno acquisire un parere formale ai sensi dell'art. 39, par. 1, lett. a), è necessario inoltrare la richiesta tramite Paleo (sistema documentale di trasmissione e protocollazione). Inoltre, per una più agevole circolazione delle informazioni ed un raccordo con lo staff del RPD sono costituiti un gruppo di lavoro di coordinamento ed una rete composta da almeno un dipendente per ciascuna struttura (Servizio e P.F.).
In base al principio di responsabilizzazione di cui all'art. 5, par. 2 del Regolamento UE, il titolare e, per suo conto, i dirigenti sono chiamati a tener traccia del percorso logico e delle motivazioni concernenti le scelte effettuate per la tutela della privacy. A tal fine è individuata una voce unica di titolario per la classificazione dei documenti nel sistema di protocollo documentale regionale
Tutta la documentazione in materia di privacy e la relativa modulistica è disponibile per tutti i dipendenti sul sito intranet Point nella sezione Organizzazione dell'Ente – Tutela dei dati personali
- Gestione delle autorizzazioni all'accesso ai dati;
- Interventi posti in essere per la formazione del personale;
L'RPD è stato cofirmatario di una nota rivolta a tutto il personale (id 14020330 del 01/06/2018) mirante a dare una prima informazione circa le novità introdotte dal citato Regolamento e contenente uno schema di informativa aggiornata alle novità introdotte dal Regolamento comunitario
La Scuola regionale di formazione della P.A., confrontandosi a tal fine con il RPD, è chiamata a predisporre una formazione obbligatoria per il personale regionale coinvolto a vario titolo nella gestione dei dati personali (referenti o esperti del trattamento, personale di supporto al RPD, addetti alla sicurezza informatica e addetti al trattamento).
La formazione è stata erogata, attraverso la Scuola regionale di formazione della P.A. che, nel 2018, ha messo a disposizione un primo corso base concernente le novità del GDPR, rivolto a dirigenti, referenti per la privacy e funzionari, nel 2019 ha implementato notevolmente l'attività prevedendo due interventi destinati allo staff del DPO e ai funzionari di altre strutture che hanno un ruolo particolare all'interno del sistema regionale di protezione (es. organizzazione e personale e informatica) strutturati con riferimento agli aspetti pratici dell'attuazione delle disposizioni del GDPR ed alla sicurezza informatica.
Nel 2020 la formazione vuole raggiungere il maggior numero di dipendenti ed è erogata in modalità e-learning
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici
Il Registro dei trattamenti è ospitato all'interno di un sistema informativo disponibile sulla intranet al seguente link: http://trattamentiprivacy.intra/; il dirigente della P.F. Informatica e crescita digitale fornisce le indicazioni operative di utilizzo secondo quanto disposto dall'art. 8, comma 4 dell'Allegato alla DGR 1504/2018. Il Registro dei trattamenti rappresenta lo strumento correlato all'analisi dei rischi che ciascun dirigente, in qualità di delegato del titolare, è chiamato ad effettuare. Il Registro inoltre è la base conoscitiva per l'attività di sorveglianza di competenza del Responsabile della Protezione Dati (RPD). Nel dettaglio si riporta quanto previsto all'art.8 della DGR 1504/18.
Art. 8 -Registro dei trattamenti
1. Il Registro delle attività di trattamento, di cui all'art. 30 del RGPD, è tenuto in formato elettronico.
2. Il Registro ha la funzione di descrivere i trattamenti effettuati all'interno della Giunta della Regione Marche. I contenuti minimi del Registro dei trattamenti sono riportati nell'allegato 1 delle presenti misure organizzative.
3. Ciascun dirigente, relativamente ai trattamenti di propria competenza, è tenuto ad aggiornare tempestivamente le informazioni contenute nel Registro mediante l'inserimento dei dati e la validazione degli stessi.
4. La gestione e manutenzione informatica del Registro è affidata alla struttura competente in materia di informatica, che assicura e fornisce le indicazioni operative di utilizzo.
5. Il Registro deve porsi come strumento correlato all'analisi dei rischi che il dirigente delegato è tenuto ad effettuare per i trattamenti di propria competenza. Pertanto l'applicativo che gestisce il Registro dovrà prevedere, oltre ai contenuti di cui all'allegato 1, le informazioni relative alle misure di sicurezza dei dati che concorrono alla valutazione del rischio. A tal fine la struttura che gestisce il Registro si consulta con il RPD.
6. Ogni responsabile esterno del trattamento detiene e rende disponibile un registro conforme alle indicazioni dell'articolo 30, comma 2 del RGPD sul modello della scheda 3 dell'allegato 1.
7. Considerato che il Registro rappresenta la base conoscitiva per l'esercizio dell'attività di sorveglianza da parte del RPD, allo stesso è assicurato l'accesso diretto in consultazione.

In occasione dell'aggiornamento del Registro dei trattamenti occorre valutare il livello di rischio del trattamento secondo una griglia di valutazione che tiene conto della probabilità e dell'impatto, riportandone l'esito nel medesimo Registro; nel caso in cui risulti che un trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche e in ogni caso in cui sussistono le condizioni di cui all'art. 9 dell'Allegato alla DGR 1504/2018, procedere alla Valutazione di impatto ai sensi dell'art. 35 del Regolamento UE, in collaborazione con i Responsabili della sicurezza fisica ed informatica e previa consultazione del Responsabile della Protezione dei Dati;

- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")
Ciascun dirigente è tenuto ad accertarsi che per tutti i trattamenti sia stata fornita l'informativa di cui all'art. 13 del Regolamento UE e regolarizzare eventuali situazioni in cui la stessa non sia conforme al nuovo Regolamento UE., secondo il modulo tipo definito. Nel caso di procedure di selezione del contraente, l'informativa concernente il trattamento dei dati del legale rappresentante e di altre persone fisiche ai sensi dell'art. 6, par. 1, lett. b) del Regolamento UE deve essere fornita in sede di bando, in conformità alla formulazione tipo di clausola
- In caso di contitolarità del trattamento, sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679
Qualora il trattamento sia effettuato in tutto o in parte da un soggetto esterno il dirigente verifica se si tratta di una situazione di contitolarità (art. 26 Regolamento UE) o se lo stesso tratti i dati per conto della Regione Marche e si configuri dunque come Responsabile esterno (art. 28 del Regolamento UE). Nel primo caso occorre sottoscrivere un accordo di contitolarità. Nel secondo caso è necessario procedere formalmente alla nomina a Responsabile del soggetto esterno, al quale devono essere fornite istruzioni per iscritto al fine di garantire che il trattamento sia eseguito in conformità al Regolamento UE e vigilare successivamente sull'osservanza delle stesse. A tal proposito si precisa che la verifica va effettuata sia sui trattamenti in essere, al fine di regolarizzare gli stessi (secondo un modello tipo di atto integrativo), sia sui trattamenti non ancora avviati. In quest'ultimo caso, qualora si preveda che il trattamento verrà affidato, in tutto o in parte, ad un Responsabile esterno da individuarsi mediante procedura di selezione del contraente, è opportuno fare menzione in sede di bando e/o nello schema di contratto che l'aggiudicazione comporterà la nomina a Responsabile esterno ed allegare alla documentazione di gara uno schema di atto di nomina redatto in conformità del citato modello. In sede di valutazione dell'offerta tecnica occorre verificare che l'operatore economico presenti le garanzie sufficienti a mettere in atto misure tecniche ed organizzative adeguate ai sensi dell'art. 28, paragrafi 1 e 5 del Regolamento UE. Le informazioni relative alla contitolarità ed al responsabile esterno devono essere inserite nel Registro dei Trattamenti.
Si riporta nel dettaglio quanto previsto all'art.5 dalla DGR 1504/18
Art. 5 - Responsabile esterno del trattamento
1 II Titolare o il dirigente delegato può avvalersi, per il trattamento di dati, di responsabili esterni del trattamento, cioè soggetti pubblici o privati con i quali, siano stipulati convenzioni o contratti in forma scritta, che specifichino la finalità perseguita, la tipologia dei dati da trattare, la durata e le modalità del trattamento, gli obblighi e i diritti del citato responsabile esterno.
2 Negli atti che disciplinano il rapporto tra l'Amministrazione ed il Responsabile esterno del trattamento devono essere presenti i contenuti indicati nell'art. 28, paragrafo 3 del RGPD.
3 II Responsabile esterno del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
4 Per quanto riguarda i trattamenti per cui i dirigenti delle strutture della Giunta regionale sono nominati responsabili esterni, da soggetti terzi, si richiama il comma 3, art. 28 del RGDP relativo agli adempimenti in capo al responsabile del trattamento.
- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati;

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione;
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati;
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno del ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Con riferimento ai temi citati negli ITEMS di cui sopra si riportano di seguito le indicazioni complessive di misure tecniche previste e prescritte dalla competente struttura regionale:
- Domicilio informatico-digitale identità digitale e posta elettronica
L'Amministrazione Regionale mette a disposizione dei Collaboratori sia caselle di posta di tipo condiviso, quali amministrazione@organizzazione.it, oppure xxx.regione@organizzazione.com, ma anche alle caselle di posta nominali quali nome.cognome@organizzazione.it.
Nel caso in cui il collaboratore, per cessazione del rapporto di lavoro o di collaborazione o per qualsiasi altro motivo, non svolga più attività all'interno dell'Amministrazione Regionale, quest'ultima manterrà la casella di posta del collaboratore attiva per un mese, previa modifica della password di accesso. In tali casi verrà impostato un messaggio automatico in cui siano fornite tutte le indicazioni utili e, in particolare, il recapito mail del collaboratore di riferimento in sostituzione.
Decorso un mese, l'account verrà disabilitato, disattivando anche il messaggio di risposta automatica.
L'Amministrazione Regionale potrà accedere ai contenuti della casella di posta disattivata per un periodo massimo di 3 mesi.
- Installazione ed utilizzo dei SoftWare
È vietato l'utilizzo/installazione di qualsiasi software/applicazione non precedentemente autorizzato dalla struttura competente in materia informatica.
In caso di installazione di software pericolosi o con licenza non regolare, rilevati all'interno delle macchine di proprietà dell'organizzazione, sarà effettuata una immediata rimozione degli stessi, valutando sia eventuali sanzioni disciplinari, sia segnalazioni alle autorità nei casi più gravi.
- Tutela riservatezza, integrità, disponibilità e resilienza della rete telematica – Backup
Al fine di garantire riservatezza, integrità, disponibilità e resilienza della rete telematica regionale, delle singole postazioni dell'ente e della server farm sono stati installati ed attivati strumenti generali di difesa informatica per:

- adottare un controllo degli accessi logici (in ingresso ed in uscita);

- garantire solo l'accesso autorizzato alle risorse informatiche;
- utilizzare sistemi ridondanti a diversi livelli per garantire continuità nell'erogazione dei servizi;
- integrare politiche di backup e verifica del disaster recovery periodiche;
- adottare misure tecniche ed organizzative per minimizzare le interruzioni di servizio.
- Implementare una topologia di rete che effettua delle partizioni logiche dei diversi ambienti;
- controllare nominalmente i criteri di accesso alla struttura di rete tramite VPN.

I pc collegati alla rete regionale sono adeguati automaticamente agli ultimi aggiornamenti critici e di sicurezza, sia per il sistema operativo che pRe le applicazioni di office.

L'utente che si collega alla sua postazione di lavoro non può avere i diritti di amministratore locale. Attraverso l'utilizzazione di appositi software centralizzati, sono individuate, da remoto, eventuali anomalie ed irregolarità, autorizzando i soggetti competenti (amministratori di sistema, tecnici autorizzati e referenti informatici):

- a disinstallare i software non autorizzati o privi di regolare licenza;
- eliminare eventuali amministratori locali e a togliere i diritti di amministratore locale se presenti;
- in caso estremo, isolare postazioni che dovessero risultare anomale o non regolari.

- Amministratori di Sistema

Sono individuati e rivisti periodicamente gli elenchi degli amministratori di sistema, alle competenze ed alla validità dei requisiti di accesso relativamente alle singole postazioni dell'ente ed alla server farm, ad eccezione dei trattamenti affidati a responsabili esterni che provvedono direttamente per competenza.

- Log degli accessi

Tutti i sistemi informatici interni sono configurati per effettuare dei LOG sulle attività e sulla connettività al fine primario di tutelare la sicurezza informatica dell'ente regionale. Tali sistemi di registrazione includono gli accessi ai sistemi, alla posta elettronica, alle connessioni di rete verso sistemi interni, alle connessioni di rete verso host esterni, all'utilizzo di file all'interno delle cartelle condivise, ecc.

- Separazione dati anagrafici e particolari - pseudonimizzazione, cifratura, minimizzazione

Nel rispetto della disciplina in materia di tutela dei dati personali a fronte di richieste specifiche da parte dei dirigenti delegati, viene dato supporto per verificare e segnalare che i fornitori assicurino la separazione tra dati anagrafici e dati appartenenti a categorie particolari dei software operativi e dei programmi applicativi, ovvero la cifratura dei dati idonei a rivelare lo stato di salute e la tracciabilità dell'attività degli utenti.

La P.F. Informatica supporta ciascun dirigente delegato al trattamento nell'adozione, se necessario, di misure di pseudonimizzazione, cifratura, minimizzazione ed in ogni altra tecnica di anonimizzazione dei dati trattati, con riferimento anche al parere 10/04/2014 del gruppo ex art.29 della direttiva 95/46.

- Verifica adeguatezza al principio della "Privacy by design"

Nel rispetto della disciplina in materia di tutela dei dati personali potranno essere valutate a campione o a fronte di richieste specifiche da parte dei dirigenti delegati, l'adeguatezza dei progetti rispetto ai principi dell'art.25 del RGDP ("Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita") nonché alla conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione.

- Accesso alla rete informatica

L'accesso alla rete informatica Interna, che è e deve essere sempre protetto da password, è limitato ai collaboratori e agli altri soggetti espressamente autorizzati dall'Amministrazione regionale con il supporto della struttura interna competente in materia ICT interna.

L'autorizzazione all'accesso al sistema informativo è data dalla struttura ICT interna. Nessuno al di fuori della stessa è autorizzato a rilasciare accessi o password atti ad accedere a qualunque sistema, compreso il Wi-Fi per gli ospiti.

Username e password per accedere alla rete ICT interna o a risorse digitali in qualsiasi forma, sono strettamente personali e il collaboratore è tenuto a tutelare e a mantenere la segretezza delle proprie credenziali di accesso.

La prima password di accesso viene fornita all'utente direttamente dal sistema ICT. Tale password dovrà essere cambiata al primo accesso da parte dell'utente stesso, secondo le regole di cui al successivo punto, e viene custodita secondo le modalità più opportune definite dallo staff ICT.

- Accesso alla rete fisica

Tutte le postazioni di lavoro collegate alla rete fisica della Regione Marche devono utilizzare un insieme di servizi di rete (Microsoft Active Directory su dominio "regionemarche.intra") per garantire il rispetto di criteri di gruppo, una gestione delle autenticazione alla rete aziendale centralizzata e la distribuzione automatica degli aggiornamenti, delle politiche di sicurezza e dei software antivirus ed antimalware.

La policy di accesso al dominio prevede l'attivazione automatica della complessità della password e della scadenza forzata ogni 85 giorni.

Per evitare attacchi "brute force" è stato introdotto il "lockout" dell'utente dopo 25 tentativi di inserimento della password.

- Regole di "Password Change"

Il Collaboratore è tenuto a sostituire la propria password ogni volta che sospetta che la stessa non sia più segreta. La password deve essere cambiata almeno una volta ogni 85 giorni.

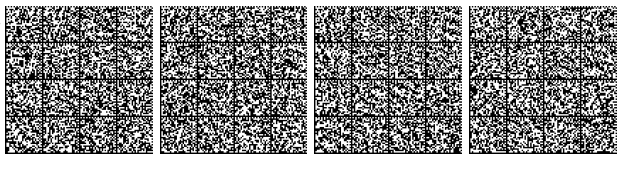
Le password devono essere formate da lettere (maiuscole o minuscole, con rilevanza ai fini del sistema), numeri e i caratteri speciali; devono essere composte da almeno otto caratteri alfanumerici di cui almeno un numero, una lettera maiuscola e una lettera minuscola e non devono contenere riferimenti agevolmente riconducibili al soggetto interessato.

Le password non devono contenere nomi o parti di nomi comuni (es. pippo, giova, maria ecc.), sequenza di caratteri troppo semplici (es ABCD, QWERTY, 12345 ecc.) o riferimenti alla propria sfera personale (es. Data di Nascita, parti del codice fiscale, nomi dei figli ecc.).

- Regole di disattivazione

Le credenziali di autenticazione non utilizzate da almeno tre mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, organizzativa o di servizio; anche in questo caso la struttura competente in materia ICT si fa garante della gestione degli account tecnici utilizzati.

Le credenziali sono disattivate anche in caso di "perdita della qualità" che consente al collaboratore incaricato l'accesso alle informazioni (per "perdita della qualità" si intende il deterioramento o perdita di caratteristiche essenziali della accoppiata "*login* + *password*" quali, ad esempio, segretezza, univocità, robustezza password, ecc. ecc.)



La cessazione degli utenti di dominio dovrà avvenire in maniera puntuale. Per gli Utenti di tipo "dipendente" (in possesso di matricola dipendente fornita dal Servizio Risorse Umane), la cessazione avviene in automatico grazie alla sincronizzazione del database delle Risorse Umane con il servizio di autenticazione di dominio.
Per gli Utenti di tipo "collaboratore/consulente" (senza matricola dipendente), a cui sono state fornite le credenziali di dominio per l'accesso alle risorse di dominio (cartelle condivise su Ormadfs, caselle di posta generiche, accesso a database e ad applicativi quali Paleo, Openact ecc.), in caso di cessazione del rapporto di collaborazione/consulenza, il Dirigente è obbligato ad avvisare immediatamente la struttura competente in materia ICT per l'immediata disattivazione dell'utente.
Il Dirigente deve porre la massima attenzione nel momento in cui: o per effetto di una riorganizzazione o per lo spostamento di dipendenti da una struttura a un'altra, le autorizzazioni precedentemente assegnate all'utente alle risorse di dominio quali caselle di posta generiche/ufficiali, cartelle condivise (OrmaDfs), accesso a banche dati o applicativi quali Paleo, OpenAct ecc. vengano modificate opportunamente tramite l'apposita modulistica messa a disposizione dalla struttura competente in materia ICT
- Custodia delle risorse
Le Risorse ICT interne non devono essere lasciate incustodite durante una sessione di trattamento dei dati. L'accesso alla postazione di lavoro deve essere bloccato ogni qual volta ci si allontani da essa (digitando sulla tastiera "CTRL+ALT+CANC"). La protezione del sistema interviene comunque in automatico dopo il periodo di inattività stabilito dalle policy. Il sistema deve essere sempre sotto controllo.
Al termine della giornata lavorativa, in caso di assenze prolungate o in caso di suo inutilizzo, il PC e le relative periferiche (monitor, stampanti ecc.) devono essere spenti.
- Cessazione del rapporto di lavoro
Al momento della cessazione del rapporto lavorativo il dipendente ha l'obbligo di riconsegnare immediatamente tutti gli strumenti e risorse ICT nello stato in cui gli sono stati consegnati, fatto salvo il normale deterioramento dovuto all'uso.
- Obbligo di condivisione ed informazione
Tutto il personale, a qualsiasi livello, e tutti i collaboratori hanno l'obbligo di comunicare al proprio responsabile e/o alla struttura competente in materia ICT, azioni, situazioni, rischi, procedure (interne e/o esterne), stati di fatto, interazioni, attività o altro che possano comportare un rischio per la sicurezza e la riservatezza dei dati e delle informazioni.
- Copia delle informazioni e gestione supporti strumenti portatili
La copia dei dati personali e di informazioni deve essere effettuata con modalità che ne garantiscano la sicurezza e secondo criteri di assoluta necessità.
L'Amministrazione Regionale mette a disposizione una struttura di "repository" ovvero di "magazzino" per le informazioni e per i dati tale per cui ne siano garantite:

- riservatezza (garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate);
- integrità (salvaguardia dell'accuratezza e della completezza);
- disponibilità (garanzia che gli utenti autorizzati abbiano accesso alle informazioni ed alle risorse associate solo quando ne hanno bisogno).

È vietato di copiare, trasferire, o muovere file dai server o NAS interne su PC portatili o supporti removibili tranne che per esigenze eccezionale e solo se espressamente autorizzato da figure dotate degli opportuni poteri amministrativi (in tal caso, l'autorizzazione deve essere accompagnata da indicazioni utili per la sicurezza delle informazioni).
- Politica del "Clean Desk" e "Clean Desktop"
I Collaboratori, nello svolgimento della propria attività devono uniformarsi a regole di "Clean Desk" e "Clean Desktop"
- Navigazione Internet
È vietata la navigazione sulla rete internet per scopi diversi da quelli strettamente legati all'attività lavorativa, sia attraverso le Risorse ICT, sia attraverso connessioni Internet personali.
È vietato scaricare da siti internet software *freeware* e *shareware*, file musicali e video
- Collegamento a rete Wi-Fi pubblica
In conformità con l'art. 8-bis "Connettività alla rete Internet negli uffici e luoghi pubblici" del Decreto Legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" e sue modificazioni, Regione Marche ha creato una rete ad accesso libero per ospiti (guest).
L'utilizzatore può collegarsi in maniera automatica per la sola navigazione Internet alla rete Wi-Fi . Al primo collegamento il sistema invia all'utente un codice di attivazione via SMS tramite il quale è possibile l'accesso alla rete. Al fine di preservare la sicurezza della rete interna da questa tipologia di accessi, le due reti restano completamente separate.
- Collegamento a rete ICT interna
Il Collaboratore può collegare un suo dispositivo, anche mobile (come lo smartphone) alla rete interna solo a seguito di una esplicita autorizzazione della funzione ICT.
Nel caso in cui gli utenti abbiano configurato posta elettronica e altre app fornite dall'ente sui propri supporti mobile (smartphone, tablet ecc.), dovranno obbligatoriamente proteggere l'accesso al dispositivo con credenziali o PIN.

Regione Piemonte

MISURE ORGANIZZATIVE E TECNICHE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati);
- Gestione delle autorizzazioni all'accesso ai dati;
- Interventi posti in essere per la formazione del personale;
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici;
- Conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto;
- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi;
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati");
- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati;

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei;
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati**;**
- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione;
- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati;
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Tutte queste misure sono attuate secondo le D.G.R. 1-6847 del 18/05/2018, D.G.R. 1-7574 del 28/09/2018, D.G.R. 1-192 del 09/08/2019.
Le misure di protezione dei dati gestiti informaticamente sono garantite principalmente dal CSI-Piemonte ente nominato responsabile esterno dei trattamenti.
Le informazioni agli interessati sono pubblicate nelle "Note legali e privacy" del sito della Regione Piemonte.

Regione Puglia

MISURE ORGANIZZATIVE
- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati) di cui alla deliberazione della Giunta regionale n. 145 del 30/01/2019 avente ad oggetto "*D. Lgs. 10 agosto 2018, n. 101 - nomina dei designati al trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti determinati)*"
- Gestione delle autorizzazioni all'accesso ai dati;
- Interventi posti in essere per la formazione del personale;
- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici;
- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati");
- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati;

MISURE TECNICHE
- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi;
- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro;
- Utilizzo di tecniche di cifratura e/o pseudonimizzazione;
- Adozione di misure per garantire la qualità e la correttezza dei dati;
- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679;
- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto);
- Modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche;
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni.

Regione Siciliana

MISURE ORGANIZZATIVE
La Regione Siciliana si è dotata di un proprio modello organizzativo per il trattamento dei dati personali in conformità al GDPR con l'approvazione della delibera di Giunta n. 483 del 29/11/2018, dopo avere individuato, con delibera n. 203 del 23/5/2018 un unico DPO per i propri uffici.
In particolare la delibera di Giunta n. 483/2018:
- ha approvato le prime istruzioni organizzative e tecniche per il trattamento dei dati personali nelle quali si identificano le figure organizzative e i processi principali connessi al Regolamento 679/2016;
– ha adottato la procedura di risposta ad una violazione dei dati personali;
- ha introdotto il questionario di autovalutazione che ciascuna struttura di massima dimensione della Regione deve compilare semestralmente per valutare la propria compliance al GDPR;
- ha istituito la figura del Referente privacy, per coadiuvare il Responsabile e il Titolare nell'esecuzione dei principali compiti in attuazione delle politiche di protezione dati.

Con D.P.Reg n.12 del 2019 è stato meglio definito il modello organizzativo, istituendo una struttura intermedia presso il Dipartimento della Funzione Pubblica e del Personale con il compito di supportare il DPO nello svolgimento delle sue funzioni, pur mantenendo, quest'ultimo, la necessaria autonomia ed indipendenza operativa e il suo diretto riferimento al vertice gerarchico dell'Amministrazione.

MISURE TECNICHE
Con delibera di Giunta n. 297 del 8/8/2019, è stata approvata la delega ai dirigenti generali di alcuni adempimenti operativi degli assessori, restando esclusi in quanto non delegabili, i poteri di controllo, indirizzo e vigilanza, propri dei titolari.
Tra i compiti delegati:
– l'aggiornamento del Registro dei trattamenti, fatta eccezione per la scelta del Responsabile a cui affidare il trattamento;
– la nomina dei sub-Responsabili e dei sub-Responsabili tecnici;
- l'adozione delle misure organizzative e tecniche per garantire che il trattamento sia conforme al Regolamento, sulla base degli indirizzi

forniti dal Titolare;
– l'aggiornamento delle informative agli interessati sui dati trattati;
- l'attività necessaria a garantire il diritto d'accesso dell'interessato ai dati che lo riguardano, l'informazione sui suoi diritti (rettifica o cancellazione dei dati e limitazione o opposizione al loro trattamento) e il corretto godimento dei suoi diritti.

Regione Toscana

MISURE ORGANIZZATIVE
- assetto organizzativo interno alla Regione Toscana per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati) definito da:
  1. DGR 325/2018;
  2. DGR 585/2018;
  3. DGR 521/2019;
  4. Decreto 7677/2019 (DPO);
- l'ufficio del Data Protection Officer ha definito la "Data Protection Policy" della Regione Toscana in ottemperanza del regolamento UE 2016/679, (GDPR). La Data Protection Policy è costituita da linee guida su processi e comportamenti organizzativi da attuare nel rispetto dei principi fondamentali della Data Protection by Design e by Default e dell'Accountability a tutela dei diritti e delle libertà delle persone, in riferimento a tutti i trattamenti che coinvolgono dati personali;
- accesso ai dati tramite personale autorizzato definito dalla DGR 585/2018;
- interventi posti in essere per la formazione del personale tramite:
  1. formazione in aula;
  2. formazione con la modalità on-line tramite il portale TRIO;
- monitoraggio e aggiornamento mensile del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679;
- meccanismi di certificazione: conformità allo standard ISO 27001: 2013 per l'erogazione di servizi di conservazione di documenti digitali;
- pianificati controlli interni periodici mensili
- conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto: accordo Data Protection tra titolare e responsabile del trattamento (previsto dal Decreto del DPO 7677/2019);
- registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi;
- in caso di contitolarità del trattamento, sottoscrizione di un accordo interno con il contitolare ai sensi dell'articolo 26 del Regolamento (UE) n. 2016/679: attività definite nel Decreto 7677/2019 (DPO);
- specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati sono definite da:
  1. DGR 521/2019;
  2. Decreto 7677/2019 (DPO);
- specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei sono definite dal Decreto 7677/2019 (DPO);
- specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati sono definite dal Decreto 7677/2019 (DPO).

MISURE ORGANIZZATIVE SPECIFICHE ADOTTATE PER LE ATTIVITÀ ELENCATE
TOS-00013 Studio longitudinale toscano: disuguaglianze di salute determinate da differenze socio-economiche
- informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati") sono fornite dagli enti di acquisizione dei dati;
- specifiche misure organizzative aggiuntive per garantire l'esercizio dei diritti degli interessati sono definite da: Regolamento Regione Toscana 64R/2019 (Registro Tumori).
TOS-00014 Registro di Mortalità Regionale
- informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati") sono fornite dagli enti di acquisizione dei dati (ASL);

MISURE TECNICHE
- sistema di autenticazione individuale degli utenti: utilizzo di accesso con credenziali di elevata robustezza (e.g. almeno 14 caratteri), utenze nominative e riconducibili a una sola persona con il controllo di complessità e scadenza delle password frequente gestito con strumenti automatici e con metodologia Single sign-on (SSO) utilizzando certificati digitali per l'accesso ai sistemi informatici;
- politica di controllo degli accessi: accesso degli utenti alle sole applicazioni per cui sono autorizzati. Una procedura di gestione delle utenze aziendali prevede l'uso di credenziali per l'autenticazione e l'accesso ai sistemi in ambito con prassi consolidate per la sospensione/eliminazione dell'utenza. I profili di accesso delle utenze e le limitazioni all'accesso ai vari sistemi e servizi sono definiti sulla base di prassi consolidate. Uso appropriato dei privilegi di amministratore con limitazione dei privilegi ai soli utenti che abbiano le competenze adeguate e la necessità operativa di accedere alla configurazione dei sistemi;
- sistema di tracciamento degli accessi: inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando l'indirizzo IP e le utenze di utilizzo;
- sicurezza delle postazioni fisiche di lavoro: effettuata tramite definizione e impiego di una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. Sono effettuati controlli in modo che apparecchiature, informazioni e software non vengano portati fuori dal sito centralizzato, dove risiedono i server con i dati, senza previa autorizzazione. Le informazioni sensibili su supporto removibile sono contenute in apposite casseforti ignifughe;
- sistemi perimetrali di controllo: valutazione e correzione continua della vulnerabilità. Le aree sono adeguatamente perimetrate. Ai locali interni accede solo personale autorizzato. Attivo un processo autorizzativo per richiedere configurazioni di rete (ad esempio firewall) e per i nuovi dispositivi da collegare in rete;
- presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati: utilizzate specifiche misure tramite configurazioni sicure standard per la protezione dei sistemi operativi con documentazione di hardening delle Virtual Machine. Le attività relative al trattamento di dati vengono effettuate solo dal personale addetto con autorizzazione dal responsabile del trattamento dei dati;

- misure adottate per garantire la qualità e la correttezza dei dati sono: verifica di copertura, verifica di completezza, verifica di analisi di coerenza interna e con altre fonti dei dati;
- intraprese azioni specifiche periodiche per controllare le apparecchiature contenenti i supporti di memorizzazione al fine di garantire che qualsiasi informazione sensibile venga distrutta fisicamente o sovrascritta in modo sicuro prima dello smaltimento o del riutilizzo;
- un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679 è in corso di adozione per il Decreto 7677/2019;
- vulnerabilità di sicurezza: attività di gestione della vulnerabilità sulle componenti applicative e infrastrutturali gestite dall'ICT, monitoraggio delle vulnerabilità di sistema e del security bulletins di ICT security e supervisione delle attività di patching gestite da ICT. L'attività di gestione delle vulnerabilità prevede attività periodiche di Vulnerability Assessment (VA) e Penetration Test (PT) con una pianificazione che copra tutti gli applicativi in un arco temporale di tre anni. Definizione di un processo per la gestione di tutti gli incidenti di sicurezza informatica, con ruoli e responsabilità precise e modalità di gestione a partire dalla raccolta delle informazioni, i report di vulnerability assessment, il diario delle attività di gestione, le comunicazioni da effettuare, le azioni di contenimento, le azioni di risoluzione, le investigazioni, l'analisi statistica ai fini del miglioramento continuo, le modalità di conservazione ai fini di una eventuale investigazione forense. Il processo è di input per il Data Breach Management, governato dal gruppo che gestisce la Privacy;
- ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto) definite da:
    1. Decreto 7677/2019;
    2. DGR 1118/2019;
- operazioni di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche definite dal Decreto 7677/2019
- trasmissione dei dati all'interno e all'esterno dell'Ente: trasmissioni effettuate con protezione dei supporti mediante cifratura per garantire integrità, disponibilità e riservatezza delle informazioni. Ogni trasmissione avviene in modo criptato e previa autorizzazione/autenticazione (Secure File Transfer Protocol - SFTP). La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. Attività di scambio di informazioni tra l'Ente e le parti esterne regolate dal provvedimento del Garante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" del 2 luglio 2015;
- collocazione di dispositivi aziendali (server di dati, sistemi di networking, pc, ecc.) in aree adeguatamente protette da rischi di accessi non autorizzati o minacce legate a danni accidentali;
- applicata protezione fisica contro i danni causati da incendi, inondazioni, terremoti, esplosioni, disordini civili e altre forme di disastri naturali o provocati dall'uomo e attuato quanto previsto nella normativa di sicurezza. Le aree di carico e scarico non permettono l'accesso alle aree con dati personali.

MISURE TECNICHE SPECIFICHE ADOTTATE PER LE ATTIVITÀ ELENCATE

TOS-00013 Studio longitudinale toscano: disuguaglianze di salute determinate da differenze socio-economiche

- tecniche di cifratura e/o pseudonimizzazione: applicazione di protezione crittografica dopo individuazione di dati con requisiti di riservatezza richiesti. Utilizzo di una tecnica di anonimizzazione con separazione delle informazioni anagrafiche dai contenuti informativi e creazione di id universale per non permettere l'identificazione dei soggetti analizzati.

TOS-00014 Registro di Mortalità Regionale

- tecniche di cifratura e/o pseudonimizzazione: applicazione di protezione crittografica dopo individuazione di dati con requisiti di riservatezza richiesti. Utilizzo di una tecnica di anonimizzazione con separazione delle informazioni anagrafiche dai contenuti informativi sulla mortalità e creazione di id universale per non permettere l'identificazione dei soggetti analizzati.

Regione Veneto

MISURE ORGANIZZATIVE

- Assetto organizzativo interno all'Ente per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)

La Giunta Regionale, Titolare del trattamento dei dati personali, ha nominato il Data Protection Officer (DPO), con DGR n. 473 del 10 aprile 2018 e con DGR n. 596 del 08 maggio 2018, ha formalmente approvato il nuovo assetto privacy dell'ente individuando le misure organizzative e tecniche volte ad assicurare il rispetto del GDPR e fornendo istruzioni per i trattamenti di dati personali effettuati presso le strutture afferenti.

Con la predetta DGR 596/2018 la Giunta Regionale, inoltre, ha delegato tutti i Dirigenti in servizio presso l'ente (quali soggetti designati), ognuno per la parte di propria competenza, al trattamento di dati personali effettuato nello svolgimento dell'incarico ricevuto, secondo quanto previsto dal rispettivo contratto individuale di lavoro ed ha altresì costituito un Gruppo di Lavoro GDPR (GdL-GDPR), per applicazione del GDPR, che coinvolge le diverse "Aree" che compongono l'organizzazione regionale.

Il Direttore dell'Area Programmazione e Sviluppo Strategico, coordinatore del citato GdL-GDPR, con nota formale del 18 maggio 2018, inviata alle strutture di vertice dell'Amministrazione regionale, ha comunicato formalmente l'adozione della predetta DGR n. 596/2018 a tutte le strutture regionali ed ha proposto i modelli di "lettera di autorizzazione", "nomina dei responsabili" ed "informativa privacy", suggeriti dal DPO e approvati dal GdL-GDPR.

La Giunta Regionale con DGR n. 1480 del 16 ottobre 2018 (Approvazione del documento "Regole per l'uso delle risorse ICT e dei dispositivi di telefonia mobile" in sostituzione delle norme comportamentali già approvate con DGR n. 1677 del 26/10/2016), infine, ha definito le nuove misure tecnico-organizzative per l'utilizzo degli strumenti informatici.

Il quadro organizzativo, è stato completato con la procedura per la segnalazione dei databreach (violazioni privacy), adottata con decreto del Direttore della Direzione ICT e Agenda Digitale.

L'assetto organizzativo descritto poggia ora su una piattaforma gestionale privacy, recentemente acquistata dall'Amministrazione Regionale, che consente di censire i trattamenti effettuati dalle strutture (a partire dalla Mappatura dei processi lavorativi), associare i trattamenti alle persone da autorizzare e gestire le conseguenti lettere di autorizzazione.

- Gestione delle autorizzazioni all'accesso ai dati

Le autorizzazioni al trattamento dei dati precedono l'autorizzazione all'accesso dei dati e si pongono quale requisito all'accesso. La gestione delle lettere di autorizzazione è in fase di implementazione attraverso il nuovo applicativo gestionale privacy che consentirà di monitorare la situazione complessiva dell'ente.

- Interventi posti in essere per la formazione del personale

Tutto il personale regionale sta seguendo uno specifico corso privacy, erogato in modalità e-learning, e a metà ottobre è stato completato da più di 1700 dipendenti.

- Monitoraggio e aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679; pianificazione di controlli interni periodici

Il nuovo applicativo gestionale privacy acquisito dall'ente consente di implementare le schede in tempo reale, facendo le associazioni con le persone che trattano i dati utilizzati in ogni specifico processo e consentendo di aggiornare le lettere di autorizzazione. Gli uffici del *Data Protection Officer* stanno seguendo i lavori di implementazione del registro, sorvegliandone l'avanzamento dei lavori. Il lavoro è molto complesso del lavoro a motivo dell'elevata numerosità delle schede (circa 1360).

- Adesione a codici di condotta e a meccanismi di certificazione; modalità di conferimento dell'incarico di responsabile del trattamento in caso di ricorso a società/ente esterno per effettuare operazioni di trattamento dei dati personali per proprio conto

Non sono adottati codici di condotta e/o certificazioni. I responsabili esterni sono nominati dai Dirigenti regionali in servizio presso l'Amministrazione Regionale (quali soggetti designati), ognuno per la parte di propria competenza.

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

La Giunta Regionale, Titolare del trattamento dei dati personali, con DGR nr. 1480 del 16 ottobre 2018 ha disposto le <<Regole per l'uso delle risorse ICT e dei dispositivi di telefonia mobile>> in cui ha definito regole specifiche al punto << 6.3.5 Sicurezza dei server >>.

In attuazione delle previsioni di Giunta, la Direzione ICT e Agenda Digitale ha quindi attivato un sistema di raccolta e protezione delle informazioni relative all'accesso ai dati, sistemi, reti ed applicazioni utilizzati dall'Amministrazione presso i propri server, in attuazione del Provvedimento Generale del Garante dei dati personali del 27/11/2008 (in materia di Amministratori di Sistema) come modificato con successivo Provvedimento Generale del 25/06/2009.

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Le informazioni agli interessati sono fornite dai Dirigenti regionali in servizio presso l'Amministrazione Regionale (quali soggetti designati), ognuno per la parte di propria competenza, all'atto della raccolta dei dati, prima dell'inizio del trattamento, come previsto dalla normativa.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati

Le Informative contengono i riferimenti della struttura del Dirigente delegato/designato e del data Protection Officer.

Gli interessati possono contattare il Data Protection Officer per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei

Il Titolare del trattamento dei dati personali, con DGR n. 596 del 08 maggio 2018, nell'Allegato A, punto 8), ha definito specifiche misure per i casi di Trattamenti effettuati senza l'ausilio di strumenti elettronici.

Nel modello di lettera di autorizzazione al trattamento, che ogni dipendente riceve, sono poi ricordati i comportamenti a cui sono tenuti tutti i dipendenti anche in ordine ai trattamenti effettuati su supporti cartacei.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

La Giunta Regionale, Titolare del trattamento dei dati personali, con DGR n. 596 del 08 maggio 2018, nell'Allegato A, punto 8), ha definito misure per i casi di trattamenti di dati particolari come previste dalla normativa.

MISURE TECNICHE

- Sistema di autenticazione individuale degli utenti e tracciamento degli accessi

La Giunta Regionale, Titolare del trattamento dei dati personali, con DGR n. 596 del 08 maggio 2018, nell'Allegato A, punto 7), ha disposto che il trattamento di dati personali con strumenti elettronici sia consentito solo alle "persone autorizzate", dotate di credenziali di autenticazione univoche.

Con successiva DGR nr. 1480 del 16 ottobre 2018 la Giunta ha poi disposto le "Regole per l'uso delle risorse ICT e dei dispositivi di telefonia mobile" in cui ha definito regole specifiche al punto "6.3.3 Autenticazione utenti".

In attuazione delle previsioni di Giunta, la Direzione ICT e Agenda Digitale ha quindi stabilito che l'accesso a tutti i servizi dalla medesima erogati avvenga previa procedura di autenticazione con identificazione univoca degli utenti e assegnazione delle credenziali individuali.

Tali credenziali, univoche e "robuste" (nome utente e password), devono essere mantenute riservate e custodite a cura dell'assegnatario.

Ogni password è associata esclusivamente ad un unico soggetto identificato. Le credenziali, laddove utilizzate, non possono essere assegnate ad altri Utenti, neppure in tempi diversi.

Le credenziali non utilizzate da almeno tre mesi sono disabilitate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

- Adozione di misure per garantire la sicurezza delle postazioni fisiche di lavoro

La Direzione ICT e Agenda Digitale ha emanato norme comportamentali dirette agli assegnatari delle postazioni fisiche di lavoro e volte a minimizzare l'esposizione a rischi delle postazioni di lavoro stesse. In particolare:

- le postazioni di lavoro "fisse" non devono essere trasportate al di fuori delle sedi dell'Amministrazione, *salvo specifica autorizzazione;*
- al termine dell'orario di lavoro, le postazioni di lavoro "fisse", salvo particolari esigenze di servizio autorizzate dal Direttore di struttura o di riferimento, devono esse spente;
- prescrizione di provvedere ad ancorare alle scrivanie le postazioni di lavoro, attraverso dispositivi fisici, laddove materialmente possibile.

- Adozione di sistemi perimetrali di controllo; utilizzo di tecniche di cifratura e/o pseudonimizzazione

La Regione del Veneto ha provveduto a dotare la rete regionale di sistemi di *firewalling* e di *content filtering* per la navigazione sicura.

Come misura di sicurezza per i trattamenti coinvolgenti dati personali, sono state altresì adottate misure specifiche di cifratura dei dati.

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

La Regione del Veneto, nell'implementare le applicazioni funzionali al trattamento di dati relativi a particolari categorie di soggetti vulnerabili, presta particolare attenzione all'attuazione dei principi di *privacy by design* e *privacy by default* così come definiti nel Regolamento (UE) 2016/679 *(GDPR).*

- Adozione di misure per garantire la qualità e la correttezza dei dati;

La Regione del Veneto ha definito un programma di audit dei dati (con periodicità variabile in relazione alla natura dei dati stessi) volto ad assicurare e migliorare la qualità dei dati stessi individuando le opportune azioni correttive.

- Predisposizione di un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach) ai sensi dell'articolo 33 del Regolamento (UE) 2016/679

Con Decreto n. 119 del 26 settembre 2019 il Direttore della Direzione ICT e Agenda Digitale della regione del Veneto sono state approvate le Linee Guida per la notifica della violazione dei dati personali ("Data Breach") e la relativa modulistica, in attuazione degli art. 33 e 34 del GDPR e della DGR n. 596/2018.

- Adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto)

La Regione del Veneto ha implementato un insieme di procedure di "backup" e "restore", volte a garantire la disponibilità dei dati stessi, minimizzando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella loro gestione.
- Modalità di cancellazione sicura dei dati in caso di dismissione di apparecchiature elettroniche
La Regione del Veneto, per quanto riguarda la dismissione delle apparecchiature elettroniche, implementa procedure dirette a distruggere o a rendere inutilizzabili (cancellandone il contenuto in maniera sicura) i supporti contenenti dati di natura personale, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13/10/2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali" (doc. web n. 1571514).
- Adozione di modalità di trasmissione dei dati all'interno e all'esterno dell'Ente che garantiscano l'integrità, la disponibilità e la riservatezza delle informazioni
La Regione del Veneto, al fine di garantire l'integrità, la disponibilità e la riservatezza delle informazioni, impone l'utilizzo di canali trasmissivi basati su protocolli sicuri e cifrati (es. HTTPS, IPSEC, FTPS)
Le misure di protezione dei dati gestiti informaticamente sono garantite principalmente dalla Direzione ICT ed Agenda Digitale delle Regione del Veneto.
Le informazioni agli interessati sono pubblicate sul sito della Regione del Veneto.

Provincia di Belluno

MISURE ORGANIZZATIVE
- È stato adeguato alla nuova normativa sulla privacy l'assetto organizzativo interno all'Amministrazione per la gestione della protezione dei dati personali e la definizione di ruoli e delle responsabilità dei soggetti coinvolti nel trattamento.
- Vi è una gestione delle autorizzazioni all'accesso ai dati.
- Sono stati effettuati interventi per la formazione del personale.
- Viene effettuato il monitoraggio e l'aggiornamento del Registro dei trattamenti ai sensi dell'articolo 30 del Regolamento (EU) 2016/679, e sono pianificati controlli interni periodici.
- Sono stati conferiti gli incarichi di responsabile del trattamento per i casi di ricorso a società esterne per effettuare operazioni di trattamento dei dati personali per proprio conto.
- L'accesso ai locali in cui sono posti i server è allarmato e prevede un accesso con codice su tastierino numerico. Le persone autorizzate sono registrate in un elenco.
- Sono state adottate misure specifiche per garantire l'esercizio dei diritti degli interessati.
- Per il progetto inserito nel Psn si sta predisponendo un accordo interno con le Direzioni ISTAT interessate.
- Sono state adottate misure per garantire l'esercizio dei diritti degli interessati.
- Sono state adottate delle misure in presenza di categorie vulnerabili di interessati e in relazione ad alcuni particolari dati trattati.

MISURE TECNICHE
- È presente un sistema di autenticazione individuale degli utenti e tracciamento degli accessi.
- Sono utilizzate tecniche di cifratura e di pseudonimizzazione dei dati (in particolare viene utilizzato un algoritmo di hashing)
- Sono adottate misure per garantire la qualità e la correttezza dei dati.
- È presente un sistema di monitoraggio e di segnalazione degli incidenti, degli eventi anomali e dei data breach ai sensi dell'articolo 33 del Regolamento (UE) 2016/679.
- Sono presenti modalità di ripristino della disponibilità dei dati e dell'accesso al sistema per i casi di incidente fisico o tecnico.
- Sono attive modalità di cancellazione sicura dei dati in caso di dismissione delle apparecchiature elettroniche.
- Sono state adottate modalità di trasmissione dei dati all'interno e all'esterno dell'Amministrazione che garantiscono l'integrità, la disponibilità e la riservatezza delle informazioni.
Si fa comunque presente che il progetto di cui questa Amministrazione è titolare prevede che i dati personali siano linkati già in sede ISTAT e che solo successivamente siano a noi trasmesse le tabelle dei dati. Nel caso sia necessario linkare i dati nella nostra sede essi vengono processati con un algoritmo di hashing e immediatamente dopo i dati personali sono cancellati.

Terna

MISURE ORGANIZZATIVE
- Assetto organizzativo interno per la gestione della protezione dei dati personali e la definizione dei ruoli e delle responsabilità dei soggetti coinvolti nel trattamento (soggetti designati e soggetti autorizzati a trattare i dati)
Terna ha adottato un modello di gestione dei dati personali basato su un quadro specifico di ripartizione delle responsabilità e sull'adozione di comportamenti e strumenti idonei alla loro protezione e sicurezza.
Il modello *privacy* Terna definisce l'assegnazione di specifiche responsabilità e ruoli in favore dei principali soggetti che rilevano nell'ambito del trattamento dei dati personali. In particolare, si evidenzia che:
- Titolari del Trattamento sono la Capogruppo e le Società Controllate; inoltre Terna S.p.A. e le Controllate Terna Rete Italia S.p.A., Terna Plus S.r.l. e Terna Energy Solutions S.r.l. sono Contitolari del trattamento dei dati personali in loro possesso, in virtù di specifici contratti sottoscritti per l'erogazione di servizi amministrativi e di accordi di Contitolarità.
- Terna S.p.A. e le Controllate Terna Rete Italia S.p.A., Terna Plus S.r.l. e Terna Energy Solutions S.r.l., in quanto Contitolari del trattamento, hanno designato congiuntamente la figura del Delegato Privacy alla quale è attribuito il presidio della gestione e del coordinamento di tutte le attività relative alla tutela dei dati personali trattati. Al Delegato Privacy è attribuito, tra gli altri, anche il compito di curare i rapporti con l'Autorità Garante per la protezione dei dati personali, tra cui la notifica a quest'ultima in caso di violazione dei dati personali (*data breach*), a seguito di consultazione con il *Data Protection Officer*.
- Il *Data Protection Officer* (DPO), figura presente nel modello privacy di Terna Spa e delle Società Controllate che si qualificano come Contitolari. L'attuale DPO di Terna, che ricopre anche il ruolo di Responsabile della struttura Gestione Qualità e Rischi di Terna Spa, è stato designato dal Delegato Privacy in data 10 aprile 2019 in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali, e della capacità di assolvere ai compiti previsti dalla Disciplina Privacy.

Il DPO provvede a promuovere iniziative di sensibilizzazione e/o formazione del personale (dipendenti, collaboratori, stagisti); inoltre viene tempestivamente e adeguatamente coinvolto in tutte le tematiche connesse alla protezione dei dati personali e alle decisioni che possano impattare sulla protezione dei dati.
Il DPO viene, altresì, consultato immediatamente qualora si verifichi una violazione e/o perdita di dati (c.d. "*Data Breach*") o un evento che potrebbe potenzialmente essere qualificabile come tale. Anche a tal fine, in Terna è stata attivata la casella di posta dpo@tema.it.
Infine, si segnala che, nello svolgimento del suo ruolo, il Data Protection Officer di Terna rappresenta una figura del tutto "autonoma" rispetto all'organico aziendale e alle figure di vertice e non riceve alcuna istruzione da parte dei Titolari, ma adempie ai propri compiti in maniera del tutto indipendente e imparziale.
- La struttura Data Protection & Privacy, costituita nell'ambito organizzativo di Tutela Aziendale, svolge le attività di seguito riportate nell'ambito delle Società rappresentate dal Delegato Privacy:

- assiste e supporta il Delegato Privacy nei rapporti formali con il Garante e cura i relativi adempimenti operativi (risposte a quesiti, notifica delle violazioni dei dati personali, etc.);
- monitora le finalità e le modalità dei trattamenti di dati personali, compresi quelli inerenti i Dati Particolari e Giudiziari se presenti, promuovendo e svolgendo operazioni di verifica e controllo;
- provvede a svolgere la mappatura di tutti i trattamenti di dati personali svolti nel contesto aziendale, procedendo con la compilazione del Registro delle attività di trattamento del Delegato previsto dall'art. 30 del GDPR;
- riceve e processa le istanze provenienti dagli Interessati al trattamento dei dati, e gestisce d'intesa con il Data Protection Officer e con le strutture interessate, l'attività di risposta.
- coordina le eventuali richieste provenienti dal Garante per la protezione dei dati personali, comprese eventuali ispezioni da questi ordinate tanto sulla Titolare quanto sulle Contitolari.

Per le altre Società Controllate del Gruppo Terna, considerate quali Titolari autonomi del trattamento, la struttura *Data Protection & Privacy* fornisce il proprio supporto nel coordinare i presidi locali deputati ad implementare e promuovere la compliance alla normativa in tema di Privacy.
- In virtù dell'art. 28 del GDPR, Terna, nel caso in cui decida di affidare per suo conto ad un soggetto esterno attività e/o servizi che prevedono il trattamento di dati personali, provvede alla designazione dei Responsabili Esterni del trattamento che devono attenersi agli obblighi contenuti nei *Data Processing Agreement* (DPA).
- Le "Persone Autorizzate al trattamento" sono identificate quali persone fisiche autorizzate dal Titolare a compiere materialmente operazioni di trattamento dei dati. In Terna vengono individuati e agiscono come Persone Autorizzate quei dipendenti, collaboratori, stagisti che, nello svolgimento delle mansioni lavorative loro affidate, entrano in contatto con dati personali – di varia natura e riconducibili a varie categorie di Interessati – e provvedono al loro trattamento.
- Gli Amministratori di Sistema, figura disciplinata dal Provvedimento del Garante del 27 novembre 2008 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499), sono sottoposti a nomina formale da parte dei rispettivi Responsabili organizzativi Terna e, ove si ravvisi la necessità, da parte del Delegato; sono – secondo i dettami del linguaggio informatico – figure professionali deputate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti, nonché ulteriori figure specialistiche ad essi equiparate se incaricate di mansioni equipollenti sotto il profilo dei rischi potenziali collegati con la protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
- Nell'ambito delle articolazioni aziendali che riportano al Delegato Privacy sono inoltre individuati i *Privacy Focal Point*, figure chiamate a svolgere, con riferimento alla propria articolazione aziendale, i seguenti compiti:

- censire i nuovi trattamenti di dati personali svolti, le relative modifiche o cessazioni, e trasmettere tutte le informazioni alla struttura *Data Protection & Privacy* al fine di consentire alla stessa di aggiornare il Registro delle attività dei trattamenti;
- verificare, con il supporto della struttura Data Protection & Privacy, che ogni policy e/o documentazione prodotta dalla propria struttura sia conforme alla Disciplina privacy e in particolare che le informative rivolte agli Interessati siano *compliant* a quanto dispone il GDPR;
- sostenere iniziative di sensibilizzazione, comunicazione e formazione sui temi di sicurezza dei dati personali e Privacy.

- Gestione delle autorizzazioni all'accesso ai dati
Le risorse informative aziendali devono essere accessibili in modo controllato, per prevenire accessi non autorizzati ai Sistemi Informativi aziendali o trattamenti non legittimi delle informazioni. In quest'ottica le *Policy Terna* per la gestione delle autorizzazioni all'accesso ai dati hanno l'obiettivo di formalizzare un iter comune per la corretta associazione utente/risorse, in modo da delimitare con chiarezza l'ambito delle risorse informative aziendali cui l'utente può accedere e le operazioni consentite su di esse.
Ogni singolo utente o applicazione accede alle risorse informative con un profilo di accesso da mantenere per il periodo di tempo in cui le sue esigenze funzionali lo richiedano e solo a valle di una specifica autorizzazione.
L'iter autorizzativo rappresenta un elemento cardine del controllo degli accessi finalizzato a legittimare l'entità ad accedere ai sistemi sulla base dei seguenti principi:
- Principio "*leastprivilege*", ossia accesso alle sole risorse di interesse, in base alle reali esigenze di business e, limitatamente agli utenti e/o amministratori, con quei privilegi di accesso che sono strettamente necessari allo svolgimento dei compiti assegnati;
- Principio "*need-to-know*", ossia l'autorizzazione all'accesso alle risorse informative deve essere concessa solo a coloro che ne hanno reale necessità in ragione delle attività lavorative;
- Principio "*Separation of Duties (SoD)"*, adottato nell'associazione di un utente ad un profilo; tale criterio ha lo scopo di impedire che un utente possa, con i privilegi a lui assegnati, eseguire attività valutate tra loro incompatibili in ragione del rischio derivante da violazioni, qualora queste fossero di competenza della medesima persona.

Le policy Terna prevedono che il principio di "*separation of duties*" debba essere rispettato anche nell'assegnazione dei Ruoli aziendali che implementano l'iter autorizzativo distinguendo, in particolare, chi richiede l'accesso da chi concede l'autorizzazione e da chi effettua la gestione utenze attraverso gli strumenti di provisioning degli account.
- Interventi posti in essere per la formazione del personale
A seguito dell'applicazione del GDPR, Terna si è attivata con azioni di sensibilizzazione rivolte a tutta la popolazione aziendale, in particolare attraverso l'erogazione di corsi di formazione in materia di protezione dei dati personali. In particolare, a partire da maggio 2018, sono stati erogati corsi in aula rivolti al Top Management e corsi online rivolti a Quadri e Impiegati.
Inoltre, si rappresenta che, in materia di data protection, vengono regolarmente erogati corsi online, con fruizione obbligatoria, rivolti al personale neoassunto.

Si segnala, infine, che sono altresì erogate specifiche "pillole formative"rivolte ai dipendenti che svolgono specifici trattamenti (ad es. il corso: "Privacy per gli Amministratori di Sistema").

- Modalità di conferimento delle informazioni ex articoli 13 e 14 del Regolamento (UE) n. 2016/679 ("informazioni agli interessati")

Tutte le informative privacy destinate ai dipendenti Terna sono pubblicate nel sito intranet aziendale nella sezione Comunicati al Personale. Le informative rivolte ad altre categorie di interessati (ad es.: azionisti, utenti della rete, candidati esterni alle selezioni del personale) sono pubblicate nel sito web aziendale (www.terna.it).

- Registrazione degli accessi delle persone nei locali in cui sono posti i server e le banche dati e la protezione degli stessi

Le misure per il controllo ed il monitoraggio degli accessi fisici ai sistemi informativi si attuano sia a livello di perimetro fisico dell'Area ICT (in questo caso si tratta di controlli comuni a più sistemi), sia a livello di sistema informativo o addirittura di singolo asset ICT (intendendo con ciò anche i *cabling-system*), come ad esempio quando si utilizzano armadi rack allarmati con apertura controllata.

Le Aree ICT sono preventivamente classificate in modo da garantire che ciascuna Area ICT disponga di misure di sicurezza fisica adeguate al contesto, ovvero in funzione delle minacce applicabili, e commisurate al livello di classificazione stabilito e coerenti con gli eventuali requisiti di sicurezza espressi dagli *Information System Owner* dei sistemi ospitati.

Per le Aree ICT non aziendali, in quanto non direttamente controllate da Terna, è assicurata la verifica, già in sede di contrattazione, della presenza di adeguati controlli per sono attentamente valutate per individuare le possibili misure compensative da implementare a livello di sistema o di ala protezione fisica ovvero garanzie ed evidenze sulla loro implementazione, nonché l'acquisizione delle modalità e degli strumenti per il monitoraggio della loro corretta applicazione.

Eventuali situazioni di impossibilità di implementare adeguate misure di sicurezza fisica nell'Area ICT sono attentamente valutate per individuare le possibili misure compensative da implementare a livello di sistema o di asset ICT.

In particolare, le Policy Terna di Sicurezza degli Accessi fisici ai locali che ospitano asset ICT prescrivono che tali accessi devono:

- essere regolati da criteri autorizzativi prestabiliti che siano oggetto di revisione periodica:
- essere consentiti solo alle persone autorizzate (personale assegnato all'area, persone specificamente autorizzate, ecc.);
- essere condizionati al possesso di opportune credenziali (ad esempio badge dotato di meccanismi di identificazione);
- avvenire tramite varchi controllati dotati di opportune misure di controllo dell'accesso fisico
- essere monitorati per rilevare le intrusioni, analizzando periodicamente le registrazioni degli accessi fisici e utilizzando i risultati delle analisi per migliorare la capacità di risposta agli incidenti di tipo fisico.

- Adozione di specifiche misure organizzative per garantire l'esercizio dei diritti degli interessati;

Le specifiche misure organizzative adottate da Terna per garantire l'esercizio dei diritti degli interessati sono descritte all'interno di ciascuna Informativa Privacy.

Gli interessati possono avanzare le proprie istanze scrivendo alla casella di posta privacy@terna.it

- Adozione di specifiche misure per la comunicazione o la custodia dei dati in caso di trattamenti che prevedono l'utilizzo di supporti cartacei;

Terna ha disciplinato le misure di sicurezza per la comunicazione e la custodia di tutte le informazioni aziendali, incluse quelle che utilizzano supporti cartacei. In particolare, al fine di garantire un adeguato livello di protezione alle Informazioni è stato sviluppato e adottato in azienda un modello unico di *classificazione delle Informazioni*, che permette di valutare il loro "valore" attraverso il grado di sensibilità e criticità che hanno per l'azienda, tipicamente in relazione al danno provocato da una loro distruzione, alterazione o divulgazione non autorizzata. In questa operazione, è opportuno ricondurre le Informazioni elementari a famiglie di contenuti informativi, che comprendono ad esempio i Dati Personali. Tutte le tipologie di informazioni trattate in Terna sono identificate ed assegnate ad un Information Owner che, in base alla classificazione specificata, ne determina gli attributi di sicurezza di riferimento suddividendole tra informazioni sensibili controllate (o in sigla: ISC) a basso, medio o alto impatto ed informazioni che, non avendo attributi di riservatezza, sono classificate non sensibili (o PUBBLICHE). Inoltre, sempre l'Information Owner assegna l'etichetta di classificazione raccomandata per i supporti informativi (sia informatici che cartacei) che le contengono. Nello specifico, le Politiche di Sicurezza Terna prescrivono che per la protezione delle informazioni su supporto cartaceo l'utente sia tenuto a:

- evitare accuratamente che, durante le normali attività lavorative o in caso di allontanamento dalla scrivania, eventuali documenti classificati siano visibili a persone non autorizzate;
- non lasciare incustoditi documenti classificati, proteggendoli in modo adeguato al loro livello di sicurezza (ad esempio in armadi con chiave), in occasione di assenze prolungate;
- recuperare tempestivamente i documenti classificati in formato originale o in copia, da scanner, fotocopiatrici, fax e stampanti, con particolare riferimento ai dispositivi condivisi (ad esempio stampanti di gruppo/rete).

- Adozione di specifiche misure in presenza di categorie vulnerabili di interessati o in relazione alla particolare natura dei dati trattati

Nel caso in cui si ravvisino trattamenti che comportino rischi per i diritti e le libertà degli individui, Terna effettua la *Data Protection Impact Assessment* (DPIA) in ottemperanza alle disposizioni del GDPR; si precisa, al riguardo, che Terna si è dotata di una specifica *policy* interna che stabilisce le modalità per lo svolgimento delle DPIA.

MISURE TECNICHE

TERNA, al fine di prevenire e gestire tempestivamente eventuali attacchi *cyber*, ha consolidato nel tempo il proprio modello dotandosi di una struttura organizzativa dedicata dal 1° gennaio 2018, di un corposo sistema di regole e procedure ispirate a standard nazionali e internazionali di riferimento (tra cui: NIST, Framework Nazionale per la Cybersecurity e la Data Protection, ISO 27001) e ha intensificato le iniziative formative e i progetti in tale ambito.

Nel dettaglio, nell'ambito dell'articolazione organizzativa di Terna S.p.A ed in particolare nell'ambito di Tutela Aziendale, è stata istituita le struttura *Cybersecurity & Data Protection* volta a presidiare il processo di gestione in tempo reale della sicurezza operativa logica e di protezione dei dati personali per tutto il Gruppo, attraverso lo sviluppo di strumenti e standard di cybersecurity e la verifica di vulnerabilità dei sistemi e della compliance alla normativa sulla privacy.

Il Modello Operativo di *Cybersecurity & Data Protection* supporta i principali processi in ambito ICT, garantendo principi di separazione dei compiti e associando responsabilità di governance a responsabilità di indirizzo operativo e di gestione degli eventi di *Cybersecurity*.

Centro nevralgico operativo della gestione degli eventi cyber è il *Computer Emergency Readiness Team* ("CERT"), che assicura il monitoraggio centralizzato in tempo reale della sicurezza del Gruppo e il monitoraggio preventivo e reattivo delle potenziali minacce cyber. Il CERT è anche coadiuvato da un *Security Operation Center* ("SOC") in h24 secondo un modello *co-managed*, al fine di garantire il governo costante del processo di *cybersecurity*.

Unioncamere

MISURE ORGANIZZATIVE

In premessa si fa presente che l'Unioncamere, oltre al Registro dei Trattamenti ed alla nomina di un DPO, ha sviluppato un "*Sistema di gestione privacy*" costituito da un insieme organico di documenti, tra loro correlati, che saranno indicati nel prosieguo.

- Con riferimento alle attività statistiche, si evidenzia che i due lavori statistici realizzati da Unioncamere che trattano dati personali (Imprese individuali, liberi professionisti, lavoratori autonomi e soci unici) sono i seguenti:

- l'indagine UCC – 00007 Sistema informativo per l'occupazione e la formazione, Excelsior realizzata dall'Area Formazione e Politiche Attive del Lavoro, nella quale è inserito funzionalmente l'Ufficio Statistica dell'Ente, e
- l'indagine UCC – 00003 Statistiche dell'archivio del Modello Unico di Dichiarazione Ambientale (c.d. "MUD") realizzata dall'Area Economia Circolare e Ambiente.

In entrambe le indagini non vengono trattati dati personali di soggetti vulnerabili, né dati personali particolari (ex dati "sensibili").

- L'Unioncamere, nell'ambito del citato "*Sistema di gestione privacy*", dispone di un documento "*Modello organizzativo, ruoli e responsabilità, ai sensi del Regolamento UE 679/2016*" formalmente adottato per la regolamentazione dei ruoli e delle responsabilità assegnate ai vari livelli gestionali, di controllo ed operativi, al fine di garantire la *compliance* alla normativa di riferimento. Nel documento sono indicate le modalità per il rilascio delle necessarie istruzioni ai soggetti autorizzati, ai vari livelli, al trattamento dei dati personali, nonché la gestione delle autorizzazioni all'accesso dei dati personali stessi in funzione dei ruoli e responsabilità del personale delle diverse aree/uffici/servizi; sono previsti strumenti per il monitoraggio e controllo del sistema, al fine di garantire il miglioramento continuo dello stesso ed il mantenimento di detta *compliance*.
- Nel modello sono anche definite le modalità per fornire agli interessati le informazioni ex art. 13 e 14 del GDPR che sono gestite dalle singole aree/uffici dell'Ente nell'espletamento delle loro attività.

Per quanto riguarda l'indagine UCC – 00007 Sistema informativo per l'occupazione e la formazione Excelsior, l'informativa alle imprese è fornita dal Segretario Generale su predisposizione dell'Area Formazione e Politiche attive del Lavoro.

Per quanto riguarda il Modello Unico di Dichiarazione Ambientale (MUD), l'informativa sulle finalità della raccolta dei dati è stata fornita, a tutti i soggetti tenuti alla presentazione, dalle Camere di Commercio competenti attraverso i portali telematici adibiti alla raccolta di tali dati.

In particolare, l'elaborazione statistica dei dati contenuti nel MUD, di cui all'indagine UCC – 00003 Statistiche dell'archivio del Modello Unico di Dichiarazione Ambientale, è svolta da Unioncamere in qualità di soggetto competente ai sensi dell'art. 3 comma 1 della legge n. 70/1994 per la predisposizione, l'elaborazione e la comunicazione al pubblico di una raccolta statistica dei dati acquisiti sulla base del MUD. Nell'ambito di tale compito, l'Unioncamere ha affidato alla Società Ecocerved Scarl, struttura *in house* competente per i sistemi informativi ambientali, l'incarico in qualità di responsabile esterno di svolgere le attività relative alla costituzione e pubblicazione di una raccolta statistica a partire dai dati MUD e raccolti dalle Camere di Commercio.

- La disciplina per i conferimenti degli incarichi al trattamento da parte di soggetti esterni è descritta nel documento "*Linee guida per l'allocazione delle responsabilità a soggetti esterni, ai sensi del Regolamento UE 679/2016*", che prevede le indicazioni per la gestione degli accordi di contitolarità (art. 26 del GDPR), delle nomine a responsabili dei trattamenti (art. 28 del GDPR), nonché gli altri casi di attività demandata all'esterno dell'Ente.

Per entrambi i lavori Unioncamere inseriti nel Psn, tutti i soggetti esterni all'Ente appartenenti al sistema camerale e non, che a vario titolo sono interessati nelle fasi progettuali sono incaricati fornendo apposite esplicite istruzioni nelle modalità di trattamento dei dati personali, in coerenza con quanto disposto dal Regolamento UE 679/2016. Attualmente non sono stati previsti rapporti di contitolarità.

- Le misure e le modalità per garantire l'esercizio dei diritti degli interessati sono indicate in un apposito documento, contenente la "*Procedura di gestione delle richieste di esercizio dei diritti degli interessati, ai sensi del Regolamento UE 679/2016*" in cui è stato definito, tra l'altro, anche un format per le istanze, nonché un apposito registro per l'annotazione ed il monitoraggio dei diritti assicurati agli interessati, anche al fine del miglioramento della gestione.
- Il personale Unioncamere è stato sensibilizzato e preparato sui temi relativi alla privacy attraverso specifiche attività di formazione in aula. I corsi formativi sono stati distinti per i diversi livelli di classificazione del personale, che incidono sulle autorizzazioni al trattamento.
- Il Registro dei trattamenti viene aggiornato ai sensi dell'art. 30 del Regolamento (EU) 2016/679 attraverso una apposita scheda di monitoraggio che viene utilizzata, altresì, per trasmettere i quesiti in tema privacy al DPO. È inoltre prevista la pianificazione dei controlli interni periodici, che rientra nel Piano della Qualità dell'Ente.
- Tra le altre misure organizzative adottate dall'Ente in materia di privacy, si segnala l'accesso vigilato delle persone (appositamente incaricate) nei locali in cui sono posti i server e le banche dati e la predisposizione di un "*Disciplinare tecnico per le funzioni di amministratore di sistema*" dal quale dipendono gli accreditamenti all'accesso delle banche dati/server e della strumentazione informatica/telematica di proprietà dell'Ente.

Data la configurazione "a rete" del sistema camerale, l'Unioncamere gestisce alcune attività – i cui server sono presso il data center di Padova – con il supporto tecnico di InfoCamere Scpa, che è la società consortile *in house* del sistema camerale. InfoCamere Scpa è nominata responsabile del trattamento ed amministratore dei sistemi Unioncamere residenti presso il data center, nonché per i profili di sicurezza relativi all'accesso ad Internet ed alla tutela contro le intrusioni telematiche.

I trattamenti di dati personali che prevedono l'utilizzo di supporti cartacei sono sempre più limitati, in ossequio all'obbligo di digitalizzazione prevista per gli enti pubblici dalla disciplina in vigore. Nei suddetti casi, la tutela della privacy viene garantita attraverso la conservazione in luoghi sicuri e protetti di documentazione contenenti dati personali con accessi limitati a persone appositamente incaricate e/o delegate.

- Con specifico riferimento alla valutazione dei rischi, l'Ente dispone di un documento su "*Linee guida per la realizzazione di una valutazione di impatto del trattamento di dati (DPIA)*" descrittivo di tutte le fasi del processo dalla valutazione e analisi del rischio fino alla formalizzazione degli esiti agli *stakeholders*, consultazione delle autorità e procedure di riesame. La valutazione è realizzata attraverso un applicativo Excel.

MISURE TECNICHE

Le principali misure tecniche adottate dall'Ente sono descritte nel documento "*Disciplinare tecnico per l'utilizzo degli strumenti informatici, telematici e principali misure di sicurezza*.

Tra i diversi temi regolamentati si segnalano: la definizione di un sistema di autenticazione e gestione delle credenziali di accesso ai sistemi informatici, protezione delle postazioni di lavoro, sistemi di salvataggio e procedure di cancellazione, modalità di gestione degli archivi informativi relativi a dati particolari (ex "*sensibili*"), modalità e procedure per un corretto utilizzo della posta elettronica e di internet,

procedure in caso di malfunzionamento, danneggiamento, smarrimento o furto dei dispositivi e degli strumenti informatici aziendali, modalità di cancellazione sicura dei dati, nonché il regime progressivo dei controlli con le relative sanzioni.
Per quanto riguarda:
- dati personali trattati nell'ambito dell'indagine UCC – 00007 Sistema informativo per l'occupazione e la formazione Excelsior, le banche dati contenenti dati personali sono archiviati nella rete intranet dell'Ente e accessibili esclusivamente dalle unità di personale dell'Area Formazione e Politiche attive del Lavoro appositamente incaricate e/o delegate. Vengono altresì, ove necessario, adottate procedure di *pseudonimizzazione*;
- l'indagine UCC – 00003 Statistiche dell'archivio del Modello Unico di Dichiarazione Ambientale, i dati del MUD conferiti sono resi anonimi al termine del trattamento statistico. Le banche dati contenenti dati personali sono archiviati presso i server della società *in house* Ecocerved Scarl; tali dati sono accessibili solo da personale incaricato della società, la quale è anche in possesso di certificazione ISO 27001 e adotta idonee misure tecniche ed organizzative adeguate al fine della sicurezza dei dati (quali ad esempio: controlli di sicurezza fisica in modo da ridurre al minimo l'accesso a persone non autorizzate ai dati; limitare al personale l'accesso alle informazioni in base al principio di necessità; presenza di un sistema antivirus regolarmente aggiornato sui sistemi informatici non disinstallabile o bypassabile da parte del personale; i sistemi informatici sono tutti aggiornati tempestivamente quando sono disponibili correzioni a vulnerabilità evidenziate; il traffico da/a Internet alla rete interna è filtrata da firewall regolarmente monitorati; è attivo un sistema di backup che permette il recupero completo dei dati).
In particolare, per quanto riguarda le procedure di segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali l'Ente ha approvato un documento sulla "*Procedura di gestione dei data breach ai sensi del Regolamento UE 679/2016*".
L'Ente è, infine, dotato di un servizio di vigilanza e di sistemi perimetrali di controllo (videosorveglianza e accessi consentiti esclusivamente tramite badge).

22A02891

Margherita Cardona Albini, *redattore* Delia Chiara, *vice redattore*

(WI-GU-2022-SON-018) Roma, 2022 - Istituto Poligrafico e Zecca dello Stato S.p.A.

PREZZO DEI DUE VOLUMI
€ 50,00