CONFINDUSTRIA

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

(art. 30, GDPR)

GLOSSARIO

Versione aggiornata alle indicazioni fornite a Confindustria dal Garante privacy

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

(art. 30 del Regolamento Ue n. 679/2016)

GLOSSARIO

Articolo 30

Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

***

Il WP29 (v. *Position Paper related to article* 30(5), del 19 aprile 2018) si è pronunciato sulla portata dell'art. 30, co. 5 del GDPR, che esonera dall'obbligo di tenuta del registro le imprese ovvero le organizzazioni con meno di 250 dipendenti che non effettuano trattamenti "rischiosi", vale a dire trattamenti che:

1. presentino un rischio, anche non elevato, per i diritti degli interessati;
2. non siano occasionali;
3. non includano dati "sensibili" e "giudiziari".

Al riguardo, il WP29 ha precisato come le 3 citate condizioni abbiano **carattere alternativo** e come, quindi, la presenza di una sola di esse determini **anche carico di imprese e organizzazioni con meno di 250 dipendenti l'obbligo di tenere e aggiornare il registro** (si pensi, ad esempio, all'impresa con un solo dipendente che tratta i dati "sensibili" di quest'ultimo).

Tuttavia, con riferimento alle imprese e alle organizzazioni con meno di 250 dipendenti tenute alla predisposizione del registro, il **WP29 ammette alcune semplificazioni**, consentendo alle stesse di limitare la tenuta del registro ai soli trattamenti "rischiosi" individuati ai sensi dell'art. 30, co. 5 del GDPR (riprendendo l'esempio di cui sopra, in assenza di altri trattamenti rischiosi, il registro dell'impresa con un solo dipendente riporterà esclusivamente il trattamento dei suoi dati sensibili).

Organigramma

Titolare del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) che, singolarmente o insieme ad altri (**contitolare del trattamento**), determina le finalità e i mezzi del trattamento di dati personali

Rappresentante del Titolare del trattamento: la persona fisica o giuridica stabilita nel territorio dell'Unione europea, designata dal Titolare non stabilito nell'Unione affinché lo rappresenti per quanto riguarda gli obblighi previsti dal Regolamento

Responsabile della protezione dei dati (DPO): il soggetto, interno o esterno alla struttura del Titolare, che in piena indipendenza e autonomia supporta quest'ultimo in merito all'applicazione degli obblighi previsti dal Regolamento, organizza e sorveglia la gestione dei trattamenti e funge da punto di contatto per le questioni in tema di privacy. La figura è obbligatoria quando le attività principali del Titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure in trattamenti su larga scala di dati particolari (ex sensibili) e "giudiziari"

Responsabile del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) esterno alla struttura del Titolare del trattamento che tratta dati personali per conto di quest'ultimo

Sub-responsabile del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) cui il Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento di dati personali per conto di quest'ultimo. Il ricorso al Sub-responsabile deve essere preventivamente autorizzato per iscritto dal Titolare.

Delegato dal Titolare del trattamento – Referente privacy: figura facoltativa, a cui il Titolare può ricorrere a fini meramente organizzativi e che potrebbe sostituire il vecchio "responsabile interno"

Descrizione del trattamento

Ufficio di riferimento: ufficio o funzione che cura prioritariamente il trattamento

Interessato: la persona fisica identificata o identificabile cui si riferiscono i dati

Categorie di interessati: es. dipendenti, collaboratori, candidati, familiari dei lavoratori, clienti/utenti, fornitori,professionisti, soggetti terzi (da precisare se minori)

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

- **Dati comuni**: es. anagrafici (nome, cognome, data di nascita, cittadinanza, stato civile, indirizzo, qualifica professione); documenti di identità (CdI, patente, passaporto); codici di identificazione fiscale (CF, partita IVA persone fisiche); dati di contatto (numero di telefono, indirizzo e-mail, indirizzo fisico); codici identificativi lavoratori (matricola, credenziali di accesso ai sistemi informatici); coordinate bancarie (numero CC, codice IBAN); targa veicolo; dati multimediali (vide, audio); dati di navigazione internet (cookie, log, indirizzo IP); dati di geolocalizzazione; dati di profilazione.
- **Dati particolari**: es. dati idonei a rivelare l'appartenenza a partiti, sindacati, organizzazioni a carattere religioso o filosofico; dati genetici; dati biometrici; dati relativi alla salute (es. gravidanza, malattia, appartenenza a categorie protette).
- **Dati giudiziari** es. dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza (es. dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).
- **Informazioni non considerate dati personali**: es. informazioni riconducibili a un soggetto non persona fisica; numero di iscrizione al registro delle imprese di una società; indirizzo e-mail, come info@azienda.com; dati resi anonimi

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Es. Responsabile del trattamento (anche semplicemente per categoria di appartenenza), persone autorizzate al trattamento (incaricati del trattamento), imprese del gruppo, associazioni di imprese, sindacati, imprese assicurative

Legittimo interesse del titolare o di un terzo: una delle basi giuridiche del trattamento a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare. Ad esempio, possono perseguire un legittimo interesse i trattamenti effettuati nell'ambito dei rapporti B2C o dei rapporti di lavoro, le comunicazioni dei dati infragruppo per fini amministrativi interni. Affinché il legittimo interesse possa operare come base giuridica del trattamento è necessario, tra l'altro, che: *i)* il trattamento non abbia a oggetto dati "sensibili" (compresi quelli biometrici) o "giudiziari"; *ii)* non operi un'ulteriore base giuridica (es. adempimento di un obbligo legale oppure l'esecuzione di un contratto del quale è parte

l'interessato o di misure precontrattuali); *iii)* le finalità perseguite sia individuate specificamente, in modo da predisporre garanzie adeguate (es. in ambito lavorativo, il legittimo interesse del datore di lavoro può essere invocato come presupposto di liceità a condizione che il trattamento dei dati dei lavoratori sia strettamente necessario per uno scopo legittimo e conforme ai principi di proporzionalità e sussidiarietà); *iv)* prima di procedere al trattamento, sia effettuata la valutazione di impatto qualora sia effettuato con nuove tecnologie o strumenti automatizzati. Per maggiori informazioni, v. Garante privacy, Provvedimento 22 febbraio 2018, n. 121).

Garanzie per il trasferimento dei dati in un Paese extra UE: decisione di adeguatezza della Commissione europea, norme vincolanti d'impresa, clausole contrattuali standard, codice di condotta, meccanismo di certificazione, clausole ad hoc autorizzate dal Garante privacy. In via residuale e in mancanza di una decisione di adeguatezza ovvero delle altre citate garanzie, il trasferimento è ammesso, tra l'altro, se l'interessato vi abbia esplicitamente acconsentito oppure se lo stesso trasferimento sia necessario all'esecuzione di un contratto concluso con il titolare o a tra questi e un terzo a favore dell'interessato. Per maggiori informazioni sulle ulteriori condizioni per il trasferimento dei dati extra UE, v. art. 49 GDPR.

Misure di sicurezza: alcuni esempi[1]

Tecniche di cifratura e pseudonimizzazione

Sistemi di autenticazione[2]

- Credenziali di autenticazione individuate tra: *i)* codice identificativo e password esclusivi; *ii)* dispositivo di autenticazione esclusivo (es. *smart card*), più eventuale password; *iii)* rilevazione biometrica (es. impronta digitale), più eventuale password
- Assegnazione individuale (per ciascun incaricato) di una o più credenziali di autenticazione
- Istruzioni in merito alla segretezza della password e alla corretta custodia dei dispositivi
- Criteri per la creazione della password: *i)* almeno 8 caratteri o il massimo di quelli consentiti dall'applicazione; *ii)* non facilmente ricostruibile (non contiene riferimenti agevolmente riconducibili all'incaricato); *iii)* da modificare dopo il primo uso; aggiornamento periodico (es. almeno ogni 3 mesi in caso di trattamento di particolari categorie di dati, almeno ogni 6 mesi in caso di altri trattamenti)
- Criteri per il codice identificativo non riassegnabile, nemmeno in tempi diversi
- Disattivazione delle credenziali per disuso (da almeno 6 mesi), perdita della qualità del profilo di accesso

Sistemi di autorizzazione[3]

- Adozione di un sistema di autorizzazione in presenza di più profili
- Individuazione e configurazione dei profili di autorizzazione prima del trattamento e secondo necessità di uso dei dati
- Verifica esistenza dei requisiti per la conservazione dei profili (almeno ogni anno)
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (almeno ogni anno)

Protezione da accessi non autorizzati

[1] La lista fornita non ha carattere esaustivo. Inoltre, si precisa che la lista ha carattere dinamico e non statico - come è stato per l'Allegato B al Codice privacy – pertanto è necessario un costante confronto con gli sviluppi della tecnologia e l'insorgere di nuovi rischi.

[2] La funzione di autenticazione ha lo scopo di accertare l'identità dell'incaricato.

[3] La funzione di autorizzazione ha lo scopo di stabilire a quali dati l'incaricato può accedere e quali trattamenti può effettuare.

- Protezione dall'accesso abusivo ai dati: *i)* misure preventive, che proteggono le vulnerabilità e riducono l'impatto degli attacchi o li rendono inefficaci (es. *antivirus, firewall, software* anti-intrusione, reti segmentate); *ii)* misure correttive, che riducono le conseguenze degli attacchi (es. copie di *backup* dei dati, software che rilevano le intrusioni o le attività sospette); *iii)* misure deterrenti, che riducono le probabilità dell'attacco (es. registrazione dei *log*, formazione del personale); *iv)* misure investigative, che rilevano quanto avvenuto e forniscono spunto per le successive contromisure (es. test di intrusione, *audit*, analisi dei *log*)
- Prevenzione della vulnerabilità dei sistemi: aggiornamento delle *patch*
- Istruzioni per la custodia e l'uso dei supporti che contengono dati
- Distruzione o inutilizzabilità dei supporti non più utilizzati; intelligibilità dei dati in essi contenuti

Ripristino della disponibilità dei dati

Salvataggio almeno settimanale dei dati; implementazione di strategie di *backup* in funzione degli strumenti utilizzati, della quantità e della tipologia delle informazioni da salvare

Piano di *disaster recovery* e/o *business continuity*

Ulteriori accorgimenti tecnici per il salvataggio dei dati (sistemi dotati di mirroring, in RAID, di tipo hot-swap, dotati di alimentazione ridondante, sistemi in cluster)

Data Breach: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Formazione degli incaricati

Piano di formazione privacy per il personale incaricato al trattamento di dati personali: *i)* contenuto degli incontri formativi a cui si intende procedere; *ii)* calendario degli incontri svolti o previsti; *iii)* registrazione dei partecipanti agli incontri formativi; *iv)* conservazione della documentazione consegnata durante gli interventi formativi

Sistemi di custodia degli eventuali archivi fisici e/o cartacei

Procedure di monitoraggio e aggiornamento dell'efficacia delle misure e delle policy

- Verifiche della conformità ai requisiti di sicurezza e protezione dei dati personali
- Conformità alla politica di sicurezza dei dati personali
- Conformità tecnica degli strumenti elettronici

- Definizione di una corretta applicazione delle misure di sicurezza da parte di fornitori esterni (es. gestione paghe)
- Politica di responsabilizzazione dei soggetti esterni (es. predisposizione di adeguati modelli contrattuali e/o clausole contrattuali)