S.p.A.

ACOSET

L'acqua è la nostra storia dal 1911.

Acoset S.p.A.

MODELLO OPERATIVO PER LA PROTEZIONE DEI DATI PERSONALI

PROCEDURA "GESTIONE REGISTRO DEI TRATTAMENTI"

19.12.2018

ACOSET S.p.A.
L'acqua è la nostra storia dal 1911.

Sommario

1 Introduzione

L'art. 30 del GDPR introduce l'obbligo della tenuta del registro dei trattamenti, ovvero uno strumento che consente di tenere traccia di tutte le operazioni di trattamento di dati personali effettuate all'interno della singola impresa. Il GDPR esonera dall'obbligo di tenuta del registro dei trattamenti le imprese 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 o i dati personali relativi a condanne penali e a reati. Per quanto attiene ai soggetti obbligati alla tenuta del registro dei trattamenti, deve precisarsi che:

- il co. I dell'art. 30 disciplina il registro dei trattamenti del Titolare, stabilendo che ogni Titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità;
- il co. II dell'art. 30 disciplina invece il registro dei trattamenti del responsabile, stabilendo che 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.

I due registri presentano delle differenze dal punto di vista contenutistico, avendo il registro del Titolare del trattamento una portata più amplia che si estende all'indicazione delle finalità del trattamento, delle categorie di interessati e delle categorie di dati personali, delle categorie di destinatari a cui i dati personali sono stati o saranno comunicati (compresi i destinatari di paesi terzi od organizzazioni internazionali), dei termini ultimi previsti per la cancellazione delle diverse categorie di dati (ove possibile).

La Società Acoset S.p.A., al fine di adeguarsi alle previsioni sopra riportate, ha definito:

- i registri dei trattamenti di dati personali, sia in qualità di Titolare sia in qualità di Responsabile del Trattamento (ove applicabile), conformi ai requisiti del GDPR. Oltre alle informazioni obbligatorie previste dall'art. 30 del GDPR, la Società ha inserito all'interno del registro un set di informazioni aggiuntive in grado di mantenere un collegamento diretto con i principali «oggetti aziendali» (es. mappa dei processi, mappa applicativa, organigramma);
- un processo operativo per la gestione del registro dei trattamenti, articolato nelle fasi di Aggiornamento, Validazione, Firma e Archiviazione e, infine, Sviluppo del registro in funzione, ad esempio, di eventuali evoluzioni normative che comportano variazioni nella struttura del registro e/o nell'interpretazione di alcuni campi in esso contenuti.
- uno strumento a supporto della gestione del registro e del relativo processo di aggiornamento, in cui tenere traccia di tutte le modifiche effettuate ai registri dei trattamenti, con riferimento a data della modifica, trattamenti interessati e

referente interno.

2 Fasi e attività

Di seguito si riportano le fasi in cui è possibile scomporre il processo "Gestione del registro dei trattamenti", con riferimento al relativo obiettivo.

Fasi	Obiettivo
1) Aggiornamento del registro	Assicurare il costante aggiornamento del registro dei trattamenti di dati personali, con riferimento sia alle informazioni obbligatorie riportate nel Regolamento UE 679/16 sia alle informazioni aggiuntive che ne consentono un collegamento con i principali "oggetti" aziendali e ne facilitano la comprensione da parte dei referenti di business
2) Validazione del registro	Garantire una validazione, sia dal punto di vista della forma sia dal punto di vista dei contenuti, delle informazioni incluse nel registro dei trattamenti, evidenziando eventuali non conformità e implementando le opportune modifiche
3) Firma e archiviazione del registro	Assicurare, ai fini del rispetto del principio di accountability, la corretta archiviazione del registro dei trattamenti, comprensivo del tracciamento delle modifiche intercorse tra le versioni e della firma.
4) Sviluppo del registro	Assicurare, alla luce di eventuali evoluzioni normative o di specifiche direttive del Vertice aziendale/ che impattano, in maniera diretta o indiretta, sul registro dei trattamenti, una opportuna evoluzione dello stesso, sia dal punto vista della forma sia dal punto di vista dei contenuti

2.1 Aggiornamento del registro

L'aggiornamento del registro è in carico ai Referenti Data Protection e può essere avviato in seguito a:

- una specifica richiesta avanzata dal DPO che, con cadenza almeno annuale, si occupa di contattare i Referenti Data Protection per raccogliere eventuali aggiornamenti;
- una segnalazione avanzata da uno o più Referenti Data Protection in merito alla necessità di:
  - rivedere le informazioni relative a trattamenti già censiti all'interno del registro dei trattamenti (es. finalità del trattamento, responsabili esterni, soggetti autorizzati al trattamento);
  - inserire uno o più trattamenti ex novo all'interno del registro dei trattamenti come conseguenza, ad esempio, della revisione delle attuali modalità di lavoro della Funzione/Ufficio.
- una segnalazione da parte del DPO o dell'Autorità di controllo che, in seguito all'esecuzione dell'audit, ha rilevato una o più non conformità.
- un'iniziativa del DPO a fronte di un cambiamento organizzativo che comporti l'introduzione di un nuovo Servizio/Ufficio o la variazione del perimetro di attività dello stesso.

Indipendentemente dall'innesco che porta all'avvio della fase, l'aggiornamento del registro dei trattamenti coinvolge in prima battuta i Referenti Data Protection, i quali ricevono, oltre a un documento di linee guida per la compilazione del registro, l'ultima versione del registro predisposta e condivisa dal DPO - solo l'estratto relativo alla rispettiva Funzione/Ufficio - e procedono alla verifica delle informazioni relative ai trattamenti di cui sono responsabili, modificando eventuali informazioni obsolete e inserendo, ove necessario, dei trattamenti ex novo. In fase di compilazione, i Referenti Data Protection possono contattare:

- il DPO (o eventuali altri membri da lui indicati) per ricevere indicazioni utili in merito all'aggiornamento del registro;
- altri soggetti autorizzati al trattamento o referenti di responsabili esterni per raccogliere eventuali informazioni o documenti mancanti da inserire o aggiornare nel registro (es. verifica del trasferimento di dati extra UE).

I Referenti Data Protection, nel rispetto degli SLA concordati, provvedono a inviare lo stesso aggiornato al DPO, dando visibilità delle eventuali modifiche effettuate. Il DPO verifica la ricezione di tutti i contributi da parte dei Referenti Data Protection e provvede a sollecitare eventuali Referenti Data Protection di cui non sono stati ricevuti i contributi, tenendo traccia di eventuali commenti riportati e/o documenti allegati.

2.2 Validazione del registro

La validazione del registro è richiesta ogniqualvolta lo stesso è soggetto a un aggiornamento da parte dei Referenti Data Protection, che può interessare l'intero registro o solo un estratto (es. trattamenti in carico a una specifica Funzione/Ufficio). Il DPO effettua una prima analisi di alto livello dell'estratto/i del registro aggiornato/i e lo/i assegna ai Referenti Data Protection, per effettuare una validazione formale. Nello specifico:

- Referenti Risorse Umane e Organizzazione, per validare i campi di natura gestionale (processi, attività, referente interno).
- Referente Affari Legali, per validare i campi di natura giuridica (titolare, contitolare e responsabile del trattamento, finalità del trattamento, base giuridica, raccolta del consenso e relative modalità, comunicazione);
- Referenti IT e Security, per validare i campi di natura informatica (trasferimento dati extra UE, asset e misure di sicurezza).

Gli attori ingaggiati dal DPO, nell'ordine sopra indicato, procedono alla revisione dell'estratto a loro assegnato e, laddove necessario, contattano i Referenti Data Protection per avere chiarimenti in merito alle informazioni contenute nel registro o per richiedere eventuali modifiche necessarie a renderlo conforme alle prescrizioni del Regolamento GDPR. I Referenti Data Protection, laddove richiesto, provvedono a effettuare le modifiche segnalate dai soggetti coinvolti in fase di validazione e a condividere nuovamente l'estratto aggiornato. Il DPO verifica la ricezione di tutti i contributi da parte dei soggetti coinvolti, provvede a sollecitare eventuali soggetti di cui non sono stati ricevuti i contributi e, una volta completata la raccolta, provvede ad aggregare gli estratti all'interno di un unico documento. Il DPO provvede a effettuare una verifica finale di quanto riportato nel registro e, in caso di eventuali non conformità rilevate, provvede a contattare direttamente il referente interno per richiedere le opportune modifiche.

2.3 Firma e archiviazione del registro

La firma e archiviazione del registro è effettuata a seguito della validazione dello stesso. Il registro è archiviato in forma scritta, anche in formato elettronico, e messo a disposizione del DPO o dell'Autorità di controllo in caso di eventuali audit. Il Legale Rappresentante della Società appone data e firma sul registro e il DPO effettua successivamente l'archiviazione della versione validata del documento e dello storico dei cambiamenti effettuati a seguito della fase di aggiornamento o di sviluppo del registro. Qualora il registro sia tenuto in formato elettronico, il Legale Rappresentante della Società appone la firma elettronica con marca temporale al fine di garantire la validità della firma nel tempo. In seguito, il DPO notifica al DPO e ai referenti dei trattamenti l'avvenuta archiviazione del registro e le modalità di accesso e

consultazione dell'archivio. Tale archivio, oltre a contenere l'ultima versione del registro, comprende le versioni precedenti del registro, le modifiche intercorse tra le differenti versioni e le linee guida aggiornate.

2.4 Sviluppo del registro

Lo sviluppo del registro dei trattamenti, in termini di struttura e/o contenuti, può essere avviato in seguito a:

- evoluzioni del quadro normativo;
- direttive dell'Autorità di controllo;
- direttive del Vertice aziendale e/o del DPO;

Le richieste di sviluppo del registro, indipendentemente dalla fonte da cui proviene la segnalazione, sono sempre prese in carico dal DPO che, valuta attentamente la tipologia e l'impatto delle modifiche richieste, oltre alla fattibilità tecnico-economica delle stesse. In caso di valutazione positiva delle modifiche o, naturalmente, di specifici obblighi normativi, la il DPO si occupa di:

- laddove siano richieste modifiche alla struttura, effettuare le opportune modifiche alla stessa e identificare nuovi campi da inserire e/o campi da eliminare, predisponendo la nuova versione del registro e tenendo traccia delle modifiche effettuate;
- laddove siano richieste modifiche ai contenuti, anche legate all'inserimento di nuovi campi (rif. punto precedente), predisporre e condividere con i Referenti Data Protection delle linee guida, comprensive di esempi concreti, per garantire una modifica omogenea del registro.

I Referenti Data Protection, in caso di modifiche richieste ai contenuti, provvederanno a effettuare le opportune modifiche, con conseguente approvazione richiesta al DPO, seguendo il medesimo processo descritto nelle prime due fasi (rif. aggiornamento e validazione del registro). La fase di sviluppo del registro si chiude con la validazione finale del registro e con la conseguente archiviazione dello stesso, comprensivo di linee guida aggiornate per la compilazione.

3 Matrice RASCI

3 Matrice RASCI Ruolo / Fasi	Data Protection Officer	Referenti Data Protection	Soggetti Autorizzati al trattamento	Responsabili esterni del trattamento	Legale Rappresentante
1) Aggiornamento del registro	A/C	R	C	C	
2) Validazione del registro	A/R	I			
3) Firma e archiviazione del registro	A/R	I			S
4) Sviluppo del registro	A/R				

Legenda:

- A (Accountable) = colui che approva il lavoro completato e ne è pienamente responsabile (dovrebbe esservi un solo Accountable per ogni attività)
- R (Responsible) = colui che lavora al pacchetto di lavoro, possono essere più di uno nel caso di lavoro in team
- C (Consulted) = chi possiede le informazioni o le capacità per svolgere il lavoro e deve essere interpellato dai responsabili dell'attività (tipicamente una comunicazione bidirezionale)
- I (Informed) = colui che deve essere informato dello stato di avanzamento e dei risultati (tipicamente una comunicazione monodirezionale)
- S (Signatory) = chi detiene il potere di firma sull'attività.

4 Metodologia e strumenti

4.1 Registro dei trattamenti

La Società ha predisposto dei registri dei trattamenti di dati personali, sia in qualità di Titolare sia in qualità di Responsabile del Trattamento (ove applicabile), conformi ai requisiti del GDPR. Oltre alle informazioni obbligatorie previste dall'art. 30 del GDPR, la Società ha inserito all'interno del registro un set di informazioni aggiuntive in grado di mantenere un collegamento diretto con i principali «oggetti aziendali» (es. organigramma, mappa dei processi, mappa applicativa). Si rimanda ai paragrafi successivi per approfondire l'elenco dei campi del registro, obbligatori e aggiuntivi, e una guida alla lettura dei trattamenti.

4.1.1 Campi obbligatori

Campi	Descrizione
Nome e dati di contatto del **titolare del trattamento** e, ove applicabile, del contitolare	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (rif. art. 4 Regolamento UE 679/2016).
Nome e dati di contatto del titolare del trattamento e, ove applicabile, del **contitolare**	Due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento (rif. art. 26 Regolamento UE 679/2016).
Nome e dati di contatto del rappresentante del titolare del trattamento	Soggetto incaricato dal titolare del trattamento a fungere da interlocutore, in aggiunta o in sostituzione del titolare del trattamento, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

Finalità del trattamento	Finalità che si persegue attraverso il trattamento di dati personali (es. finalità contrattuali, di marketing, di profilazione, amministrativo-contabili), da esplicitare all'interno dell'apposito documento da condividere con l'interessato dal trattamento (es. Informativa Clienti).
Categorie di dati personali	Categorie di dati personali oggetto del trattamento: dati comuni[1]; categorie particolari di dati personali[2]; dati relativi a condanne penali e reati.
Categorie di interessati dal trattamento	Soggetti cui si riferiscono i dati personali oggetto del trattamento (es. candidati clienti, dipendenti, fornitori).
Termini di conservazione dei dati	Termini ultimi previsti per la cancellazione delle diverse categorie di dati.
Comunicazione (e categorie di destinatari)	Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali[3] (rif. art. 30 Regolamento UE 679/2016).

[1] Dati anagrafici; Dati di contatto; Informazioni precontrattuali; Informazioni contrattuali; Informazioni di marketing; Dati fiscali; Dati contabili; Fotografie e video; Tipologia di contratto; Qualifica e livello professionale; Retribuzione; Ammontare dei premi; Tempo di lavoro; Ferie e permessi individuali; Assenze dal servizio; Trasferimenti ad altra sede; Procedimenti e provvedimenti disciplinari; Immagini videosorveglianza; Dati raccolti tramite i sistemi di controllo accessi; (...)

[2] Dati che rivelino l'origine raziale o etnica; Dati che rivelino opinioni politiche; Dati che rivelino convinzioni religiose o filosofiche; Dati che rivelino appartenenza sindacale; Dati genetici; Dati biometrici; Dati relativi alla salute; Dati relativi alla vita sessuale/orientamento sessuale.

[3] Ci si riferisce alla comunicazione verso la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile. Le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento (rif. art. 4 Regolamento UE 679/2017).

Misure di sicurezza	Descrizione generale delle misure di sicurezza tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio.

4.1.2 Campi aggiuntivi

Campi	Descrizione
Processo (e attività)	Processo e attività aziendali nell'ambito dei quali è effettuato il trattamento di dati personali.
Base giuridica del trattamento	Fondamento su cui si basa la liceità del trattamento effettuato (es. prestazione di un consenso, esecuzione di un obbligo contrattuale, adempimento di un obbligo legale).
Referente interno del trattamento	Referente aziendale a cui è formalmente attribuita la responsabilità del trattamento, con riferimento a Società e Unità Organizzativa di appartenenza.
Categorie di soggetti autorizzati al trattamento	Persone fisiche autorizzate dal titolare o dal responsabile a trattare i dati personali.
Responsabile esterno del trattamento	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (rif. art. 4 Regolamento UE 679/2016).
Modalità del trattamento	Asset fisici (archivi) e/o IT utilizzati a supporto del trattamento.