S.p.A.

ACOSET

L'acqua è la nostra storia dal 1911.

ACOSET S.p.A.

MODELLO GENERALE PER LA PROTEZIONE DEI DATI PERSONALI

19.12.2018

(rev. 1.1 14/12/2018)

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

Sommario

1 Introduzione

1.1 Obiettivi

La redazione del presente Modello rientra nell'ambito dell'adeguamento di Acoset S.p.A. alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, entrato in vigore il 24 maggio 2016 e applicabile a partire dal 25 maggio 2018 dopo un periodo di transizione di due anni.

In tale contesto, Acoset S.p.A. si dota del "**Modello per Protezione dei Dati Personali**" ("Modello") e perfeziona il Modello attualmente in uso, basato sul Decreto Legislativo del 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*" (Codice Privacy), aggiornandone l'impianto metodologico, organizzativo, procedurale e strumentale.

A tale riguardo, si evidenzia che la società Acoset S.p.a. è già dotata del Documento Programmatico per la Sicurezza dei dati (DPS) approvato nel 2017 al quale si fa rinvio per le parti in questa sede non modificate.

1.2 Struttura

Il documento si articola nelle seguenti sezioni:

- **Sezione 2** - La sezione fornisce un elenco di definizioni e acronimi di uso frequente nel presente documento;
- **Sezione 3** - La sezione riporta le indicazioni normative in materia di protezione dei dati personali che hanno guidato le scelte di Acoset S.p.A. ;
- **Sezione 4** - La sezione introduce il modello generale per la protezione dei dati personali adottato da Acoset S.p.A.;
- **Sezione 5** - La sezione approfondisce il modello organizzativo per la protezione dei dati personali adottato da Acoset S.p.A.;
- **Sezione 6** - La sezione approfondisce il modello operativo per la protezione dei dati personali adottato da Acoset S.p.A.;
- **Sezione 7** - La sezione approfondisce il modello architetturale per la protezione dei dati personali adottato da Acoset S.p.A.;
- **Sezione 8** - La sezione approfondisce il modello di controllo per la protezione dei dati personali adottato da Acoset S.p.A..

1.3 Perimetro di applicazione

Il Modello si applica solo alla società Acoset S.p.A.

1.4 Modalità di gestione

1.4.1 Revisione

La predisposizione del Modello e ogni modifica e/o integrazione rilevante allo stesso, a seguito dell'introduzione di nuove disposizioni normative ritenute significative e/o di cambiamenti interni di varia natura, è in carico al Responsabile del trattamento previa consultazione con il Data Protection Officer (DPO).

1.4.2 Approvazione

Il Modello viene sottoposto all'attenzione del Consiglio di Amministrazione, ai soli fini della sua presa d'atto.

1.4.3 Distribuzione

Una volta completato il ciclo di verifica, validazione ed approvazione del Modello da parte del DPO, lo stesso viene divulgato dal Responsabile del trattamento e reso disponibile ad Acoset S.p.A, affinché si provveda al recepimento dello stesso negli aspetti di propria competenza.

2 Definizioni e terminologie

Categorie particolari di dati personali	Dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Sono da ritenersi particolari anche i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute nonché i dati che rivelino l'orientamento sessuale della persona.
Codice Privacy	Decreto Legislativo 30 Giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*".
Comitato europeo per la protezione dei dati	Organismo dell'Unione, dotato di personalità e rappresentato dal suo presidente che garantisce l'applicazione coerente del GDPR. È composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Data Protection Officer (DPO)	Responsabile della protezione dei dati personali. La figura costituisce il fulcro del nuovo sistema di *governance* in tema di protezione dati personali, dovendo facilitare l'osservanza delle disposizioni del GDPR, minimizzare il rischio delle violazioni e agire quale intermediario fra i vari *stakeholder* (autorità di controllo, interessati e diverse Unità Organizzative aziendali).
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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.

GDPR (General Data Protection Regulation)	Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento Generale sulla protezione dei dati).
Modello per la protezione dei dati personali (o Modello)	Insieme di scelte a livello organizzativo, operativo, architetturale e di controllo volte ad assicurare un'adeguata protezione dei dati personali di Acoset S.p.A.
Soggetti autorizzati al trattamento	Persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile del trattamento (incaricati al trattamento nel Codice Privacy).
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare del trattamento (il "Titolare")	La persona fisica o giuridica, l'autorità pubblica, il 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.
Responsabile del trattamento (il "Responsabile")	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
Gruppo di lavoro articolo 29 per la protezione dei dati (c.d. WP29)	Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva

	2002/58/CE.

3 Contesto normativo

3.1 Inquadramento

Il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679, Regolamento Generale sulla protezione dei dati personali (meglio noto come General Data Protection Regulation, di seguito: "GDPR"), direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018 dopo un periodo di transizione di due anni. Il percorso legislativo che ha portato all'emanazione del GDPR è iniziato il 4 novembre 2010, quando la Commissione europea ha elaborato una proposta di riforma della normativa in materia di protezione dei dati personali. L'obiettivo del legislatore europeo è stato duplice: da un lato, adeguare la preesistente disciplina in materia, risalente al 1995, all'evoluzione tecnologica, dall'altro creare un quadro normativo comune a livello europeo. Per perseguire questo secondo obiettivo, lo strumento giuridico prescelto è stato quello del regolamento, direttamente applicabile in tutti gli Stati membri, e non, come in passato, quello della direttiva, che necessitando di recepimento nei singoli Stati, ha creato differenze normative, a volte rilevanti, fra i singoli ordinamenti giuridici degli stati membri.

Il GDPR abroga la precedente normativa in materia, ossia la Direttiva 95/46/CE del 24 ottobre 1995, "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" con l'effetto di abrogare anche, a partire dal 25 maggio 2018, le normative nazionali emanate in applicazione di tale Direttiva, come il D. Lgs. 196/2003 ("Codice Privacy"), almeno nelle parti di diretta trasposizione della sopra citata Direttiva, ma non la Direttiva 2002/58/CE (c.d."Direttiva e-Privacy") che prevede obblighi specifici per i fornitori di servizi di comunicazioni elettroniche (e quindi, nel nostro ordinamento le disposizioni del Codice Privacy di attuazione della stessa). I provvedimenti dell'Autorità Garante, invece, non decadranno fino a quando non verranno modificati, sostituiti, abrogati, a differenza delle autorizzazioni generali sul trattamento dei dati sensibili o giudiziari, che rimarranno in vigore fino al 24 maggio 2018. Il legislatore italiano, con l'art. 13 della Legge di Delegazione n. 163, ha conferito apposita delega al Governo ad adottare, entro sei mesi dalla data della sua entrata in vigore (21 novembre 2017), decreti legislativi per adeguare la normativa nazionale alle disposizioni del GDPR. Entro maggio, quindi, la materia sarà regolata sia dal GDPR sia dal Codice Privacy modificato. Da notare, inoltre, che l'ambito di applicazione della nuova normativa, è più ampio rispetto alla precedente (tanto che si è parlato di "extraterritorialità"): il GDPR si applica, infatti, non solo organizzazioni stabilite in UE (anche se il trattamento avviene fuori EU), ma anche ad organizzazioni stabilite extra UE che offrono beni o servizi a interessati che "si trovano" in UE o che monitorano il loro comportamento all'interno dell'UE (art. 3 del GDPR).

Si rimanda al paragrafo 9.1 Normative e linee guida per maggiori dettagli in merito a normative e linee guida in materia di protezione dei dati personali in vigore alla data di predisposizione del presente documento, che comprendono anche linee-guida e documenti di indirizzo formulati dal Gruppo di Lavoro istituito ai sensi dell'art. 29 della direttiva 95/46, (c.d. WP29), organismo consultivo e indipendente.

3.2 Aspetti invariati e maggiori novità

Di seguito si riporta un quadro degli aspetti invariati o che variano solo marginalmente rispetto all'attuale assetto normativo e degli aspetti nuovi introdotti dal GDPR, che saranno opportunamente approfonditi nei paragrafi successivi.

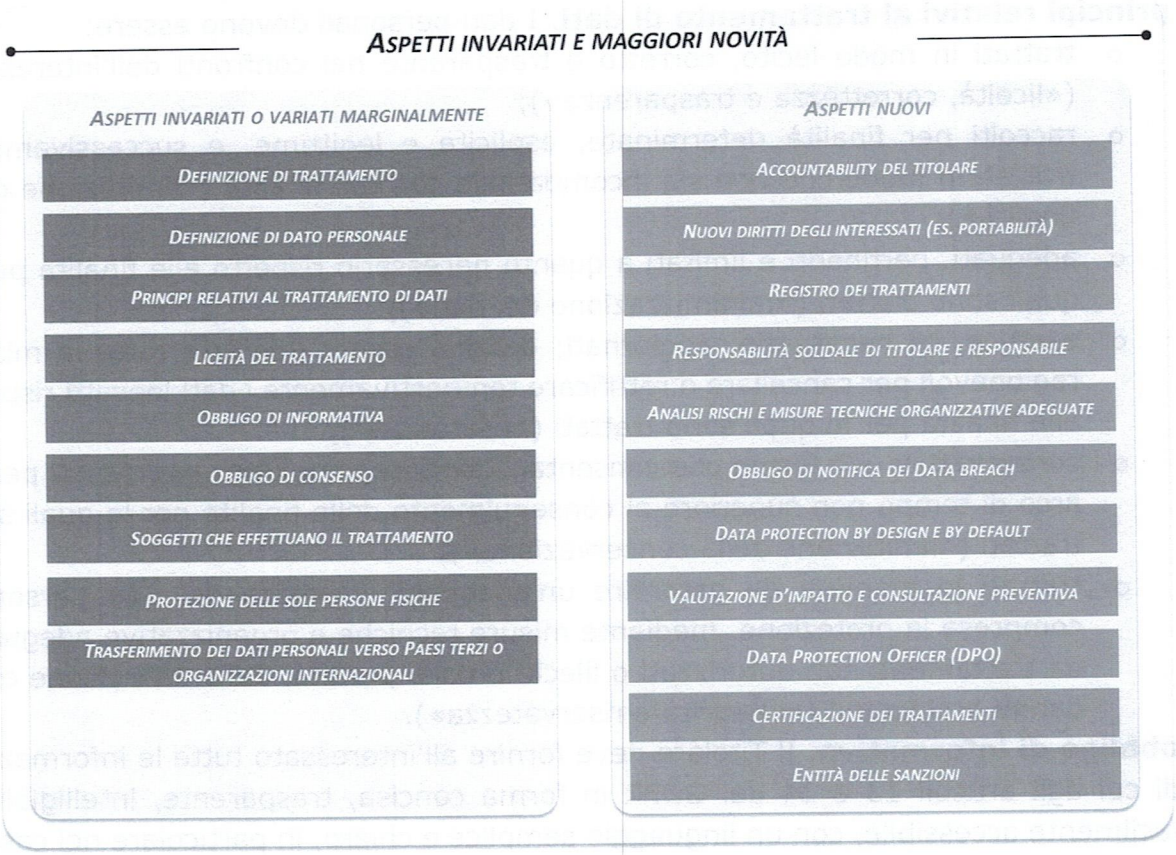

Figura 1 - Aspetti invariati o variati marginalmente e aspetti nuovi

3.2.1 Aspetti invariati o variati marginalmente

Le definizioni e i principi generali previsti dall'attuale Codice Privacy rimangono sostanzialmente invariati. In particolare, non sono variati o sono variati in maniera marginale i seguenti aspetti:

- **definizione di trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **definizione di dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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.
- **principi relativi al trattamento di dati**. I dati personali devono essere:
  - trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
  - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
  - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
  - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
  - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
  - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
- **obbligo di informativa.** Il Titolare deve fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni possono essere fornite per iscritto o con altri mezzi, anche elettronici.
- **obbligo di consenso**. Il consenso espresso dell'interessato al trattamento dei propri dati per una o più specifiche finalità nel GDPR è una delle basi giuridiche sussistendo le quali il trattamento può dirsi lecito (condizioni di liceità). Da notare che nel GDPR

il consenso costituisce una condizione di liceità al pari delle altre[1]: è posto sullo stesso piano di quelle che nel sistema italiano sarebbero le «clausole di esonero» dal consenso.

- **soggetti che effettuano il trattamento**:
  - il **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
  - il **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
  - il **sub-responsabile del trattamento**: la persona fisica eventualmente nominata dal Responsabile del trattamento, previa autorizzazione del Titolare, che tratta dati personali per conto del Titolare del trattamento;
  - gli **incaricati del trattamento**; le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal responsabile. La figura dell'incaricato non è più espressamente prevista nel GDPR, ma il Garante nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" ha precisato che le disposizioni attuali che prevedono la sua designazione sono pienamente compatibili con la struttura e la filosofia del Regolamento.
- **protezione delle sole persone fisiche**: il GDPR è volto a proteggere i diritti e le libertà fondamentali delle persone fisiche.
- **trasferimento dei dati personali verso Paesi terzi e organizzazioni internazionali**: il trasferimento di dati personali da paesi appartenenti all'UE verso Paesi "terzi" (non appartenenti all'UE o allo Spazio Economico Europeo) può avere luogo soltanto se sono rispettate le condizioni di cui al capo V del GDPR (decisioni di adeguatezza, garanzie adeguate e/o condizioni particolari).

Aspetti nuovi

Il GDPR comporta un vero e proprio cambio di filosofia: si abbandona un sistema di tipo formalistico, basato sulla previsione di regole formali, adempimenti analiticamente definiti e minime misure di sicurezza espressamente elencate per passare a un sistema di *governance* dei dati personali, basato su un'alta responsabilizzazione sostanziale («*accountability*») del Titolare del trattamento, che deve garantire ed essere in grado di dimostrare la conformità al GDPR. Tale onere probatorio si sostanzia nell'adozione di misure tecniche ed organizzative la cui adeguatezza deve essere valutata sulla base

[1] Le altre basi giuridiche previste dall'art. 6.1 del GDPR, sono adempimento obblighi contrattuali, interessi vitali dell'interessato o di terzi, obblighi di legge cui è soggetto il Titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati

delle specifiche caratteristiche dei trattamenti di dati personali (natura, ambito di applicazione, contesto e finalità del trattamento), nonché dei rischi per i diritti e le libertà delle persone fisiche (artt. 5 e 24 del GDPR). Oltre al sostanziale rovesciamento di prospettiva, il GDPR introduce anche alcune novità:

- **nuovi diritti degli interessati** (art. 17 e 20). Il GDPR introduce il **diritto all'oblio**[2] e il **diritto alla portabilità** che consente all'interessato di ricevere i dati personali forniti a un Titolare «in un formato strutturato, di uso comune e leggibile da un dispositivo automatico» e di trasmetterli a un altro Titolare del trattamento «senza impedimenti».
- **registro dei trattamenti** (art. 30). Il GDPR prevede che sia i Titolari sia i Responsabili, tranne gli organismi con meno di 250 dipendenti (a meno che si tratti di un trattamento a rischio, occasionale o riguardante **categorie particolari di dati** o i dati personali relativi a **condanne penali e a reati**), debbano tenere un registro dei trattamenti contenente almeno le indicazioni previste nel art. 30. Come precisato dal Garante privacy nazionale, nella "Guida all'applicazione del regolamento del 28 aprile 2017", si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale verifica da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda, indispensabile per ogni valutazione e analisi del rischio. Lo stesso, infatti, non costituisce un adempimento formale, bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, Il Garante invita tutti i Titolari di trattamento e i Responsabili, a prescindere dalle loro dimensioni, a dotarsi di tale registro (e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche), inserendo, se opportuno, ulteriori informazioni rispetto a quelle prescritte dall'art. 30 del GDPR.
- **responsabilità, obblighi e facoltà del Responsabile** (artt. 28 e 82). Il GDPR responsabilizza maggiormente i responsabili del trattamento rispetto al passato. Essi, infatti: possono ricevere direttamente richieste da parte dell'Autorità Garante; sono direttamente passibili di sanzioni amministrative; rispondono direttamente per il danno causato dal trattamento non solo se non hanno rispettato le istruzioni del Titolare, ma anche se non hanno adempiuti agli obblighi del GDPR specificamente diretti loro (come la tenuta del registro dei trattamenti; l'adozione di idonee misure tecniche e organizzative; la designazione di un DPO). Il responsabile risponde in solido con il titolare per l'intero ammontare del danno causato dal trattamento. Un'importante novità è la facoltà attribuita al responsabile dall'art. 28, co. 2 del GDPR di ricorrere ad un altro responsabile (di seguito: "Sub-responsabile") previo consenso scritto, specifico o generale, del Titolare, imponendo al Sub-responsabile,

---

[2] Nonostante la rubrica dell'istituto (Diritto alla cancellazione («diritto all'oblio»), l'art. 17 si limita a riprodurre, con qualche precisazione e puntualizzazione, i contorni del diritto alla cancellazione disciplinato dalla direttiva 95/46, senza tipizzare il diritto all'oblio, senza, quindi, recepire gli avanzamenti della giurisprudenza e della dottrina sulla individuazione dei connotati dell'istituto.

tramite contratto o altro atto legale, le stesse obbligazioni gravanti sul Responsabile, il quale rimane comunque pienamente responsabile per eventuali inadempimenti in materia di protezione dei dati da parte dei Sub-responsabili. In ragione della maggiore responsabilità gravante sui responsabili del trattamento, oltre alla circostanza che alcuni degli elementi contrattuali obbligatori di cui all'art. 28.3 appaiono applicabili esclusivamente a soggetti esterni (come l'impegno alla riservatezza dei propri dipendenti e collaboratori), la figura del «**Responsabile interno**» del trattamento (es. responsabile HR; IT, marketing) non appare più compatibile con il nuovo contesto normativo.

Nel futuro, pertanto, si prevede di modificare l'attuale struttura organizzativa interna, la quale individua n. 4 responsabili del trattamento interni, mediante la nomina di un responsabile del trattamento dei dati esterno all'azienda.

- **analisi dei rischi e misure tecniche organizzative adeguate** (art. 32 del GDPR) - Il GDPR non prevede misure "minime" di sicurezza, ma prescrive, in capo al titolare ed ai responsabili, l'obbligo di adottare misure tecniche ed organizzative adeguate al rischio. Per valutare l'adeguatezza delle misure, il titolare e il responsabile devono pertanto effettuare un'analisi dei rischi derivanti dal tipo di trattamento che intendono porre in essere, quali distruzione, perdita, modifica, divulgazione non autorizzata e accesso, in modo accidentale o illegale, ai dati personali trasmessi/conservati o comunque trattati. L'art 32 del GDPR elenca alcune misure, ma si tratta di un'elencazione meramente esemplificativa e non tassativa[3]: la valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati, tenuto conto non solo di natura, ambito, contesto, finalità del trattamento, ma anche stato dell'arte (evoluzione tecnologica) e costi di attuazione (elemento del tutto nuovo).
- **obbligo di notifica dei data breach** (artt. 33 e 34 del GDPR) - Il GDPR introduce l'obbligo di notificare alle autorità di controllo, senza ingiustificato ritardo (e, ove possibile, entro 72 ore), eventuali violazioni dei dati, nonché di comunicarle agli interessati senza ingiustificato ritardo laddove vi sia un rischio elevato per i diritti e le libertà delle persone fisiche.
- **data protection by design** (art. 25,1 del GDPR) - Il GDPR prevede che la realizzazione di qualsiasi progetto, servizio, sistema (sito web, software, soluzione IT, ambiente di lavoro, etc.) consideri la riservatezza e protezione dei dati personali sin dalla progettazione, utilizzando tecniche quali la minimizzazione e pseudonimizzazione.
- **data protection by default** (art. 25,2 del GDPR) - Il GDPR prevede che il titolare debba mettere in atto misure tecniche e organizzative adeguate per garantire che

---

[3] Pseudonimizzazione; cifratura; capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico¸ una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

Modello di controllo	Il modello di controllo copre le seguenti aree: - **sistema di controllo**, ovvero l'insieme di controlli in merito all'esistenza, all'adeguatezza e all'effettiva applicazione del modello per la protezione dei dati personali di Acoset S.p.A., con riferimento a tutte le dimensioni sopra indicate.

Si rimanda ai paragrafi successivi per la descrizione di dettaglio di ciascuna componente del modello per la protezione dei dati personali.

5 Modello organizzativo per la protezione dei dati personali

Attraverso la definizione di strutture, responsabili e ruoli, viene assicurato l'indirizzo e governo, l'esecuzione e il controllo del modello per la protezione dei dati personali.

Area	Strutture, comitati e ruoli
Indirizzo e governo	✓ **Titolare del trattamento (A/S)** ✓ Responsabile del trattamento (R)
Esecuzione	✓ **Responsabile del trattamento (R)** ✓ **Sub responsabile del trattamento (R)** ✓ Incaricati del trattamento (R)
Controllo	✓ **Data Protection Officer (C/I)** ✓ Autorità di Controllo (I)

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.

5.1 Indirizzo e governo

«*Indirizzare e governare*» significa garantire la definizione e il trasferimento di un modello di protezione dei dati personali compliant al Regolamento 679/2016 e alle altre disposizioni relative alla protezione dei dati. Nello specifico:

- definire linee di indirizzo del modello per la protezione dei dati personali coerenti con le scelte strategiche definite da Acoset S.p.A.;
- elaborare e trasferire un modello per la protezione dei dati personali[4] che risponda alle linee di indirizzo definite, oltre che alle disposizioni di GDPR, da calare opportunamente all'interno del settore di business;
- prendere decisioni in relazione a modifiche necessarie aventi un impatto significativo sul modello per la protezione dei dati personali, anche attraverso un'opportuna valutazione dei rischi di non conformità;
- prendere decisioni in relazione a eventuali eventi critici occorsi, quali ad esempio casi di gravi violazioni dei dati personali che possono potenzialmente comportare l'applicazione di sanzioni, perdite finanziarie rilevanti o danni di reputazionali.

La responsabilità formale dell'indirizzo e governo del Modello di Acoset S.p.A. è in carico al Titolare del trattamento, individuato nel Presidente di Acoset s.p.a., ed al Responsabile del trattamento, individuato con apposito atto di nomina.

Il Responsabile del trattamento:

- recepisce le linee guida condivise da Acoset S.p.A. e le declina opportunamente all'interno del Modello, segnalando eventuali modifiche legate al contesto di riferimento;
- sottopone il Modello all'approvazione del Titolare del trattamento, ma anche eventuali decisioni rilevanti o critiche in relazione ad eventi occorsi (es. violazioni di dati personali);
- richiede al DPO consulenze in merito al Modello (e ai requisiti del Regolamento), senza che lo stesso sia in alcun modo responsabile delle scelte effettuate da Acoset S.p.A..

5.2 Esecuzione

«*Eseguire*» significa garantire l'implementazione del modello di protezione dei dati personali definito nel rispetto, non solo delle disposizioni del Regolamento GDPR, ma

[4] Il modello per la protezione dei dati personali comprende norme di autoregolamentazione e disposizioni interne, quali ad esempio processi e regole per la gestione dei diritti dell'interessato

anche di norme di autoregolamentazione e disposizioni interne di cui si è dotata la Società. Nello specifico:

- acquisire e comprendere il modello per la protezione dei dati personali definito, ma anche le relative disposizioni del Regolamento GDPR correlate alle scelte effettuate, segnalando eventuali aspetti poco chiari
- operare secondo le disposizioni di Regolamenti interni ed esterni, sia in relazione ad attività di back office sia in relazione ad attività di front office (es. gestione richieste degli interessati)
- individuare, discutere e segnalare eventuali modifiche al modello per la protezione dei dati personali, che possono portare a benefici legati a recupero di efficienza o all'incremento dell'efficacia del modello
- supportare le attività di controllo a diversi livelli e implementare eventuali azioni correttive segnalate dalle Funzioni competenti, nel rispetto di piano di remediation definito.

La responsabilità formale dell'esecuzione del Modello di Acoset S.p.A. è in carico agli **Incaricati del trattamento** che, limitatamente ai trattamenti di propria competenza, sono formalmente responsabili dell'esecuzione del Modello.

Gli incaricati del trattamento:

- recepiscono le linee guida condivise dal Responsabile per il trattamento e le applicano opportunamente all'interno dell'Unità Organizzativa, richiedendo eventuali chiarimenti al DPO;
- sono supportati dai Sub Responsabili del trattamento, qualora individuati dal Responsabile del trattamento previa autorizzazione del Titolare, e devono operare sotto la diretta autorità delle strutture preposte dal Titolare.

Si rimanda al "Documento programmatico per la sicurezza", già adottato da Acoset s.p.a., per maggiori informazioni in merito a ruolo e responsabilità di ciascun attore, che deve intendersi allegato al presente documento.

5.3 Controllo

«*Controllare*» significa assicurare l'identificazione di non conformità del modello di protezione dei dati personali definito, sia rispetto al Regolamento GDPR sia rispetto a norme di autoregolamentazione e disposizioni interne, e l'implementazione di opportune azioni correttive nel rispetto di contesto aziendale, risorse disponibili e vincoli operativi esistenti. Nello specifico:

- Sorvegliare l'osservanza del regolamento, curando che vengano effettuati i controlli a diversi livelli in merito all'applicazione del modello per la protezione dei dati personali, ivi compreso il relativo sistema di controlli e gestione rischi;

- identificare eventuali aree di non conformità, da ricondurre al GDPR e/o regolamenti (ndr precisare quali) interni, e valutare opportunamente il livello di rischio correlato, con focus su sanzioni, perdite finanziarie o danni di reputazione;
- studiare delle possibili soluzioni da implementare per sanare le non conformità, valutandone fattibilità tecnica ed economica, e definire un piano con gli interventi selezionati, opportunamente individuati;
- monitorare l'effettiva implementazione del piano di remediation, coinvolgendo gli attori interessati per le verifiche del caso.

La responsabilità formale del controllo del Modello di Acoset S.p.A. è in carico al **Data Protection Officer**, figura introdotta dal GDPR (artt. 37-39) che: controlla e supporta l'applicazione degli obblighi della nuova normativa, fornendo anche consulenza su ambiti verticali; funge da punto di contatto con le Autorità di controllo e gli interessati per questioni connesse al trattamento.

Il Data Protection Officer:

- è supportato dai membri dell'Ufficio di staff del DPO, che si individuerà con apposito provvedimento del Titolare, per l'effettuazione di controlli in ambiti specifici e per l'effettuazione dei controlli di linea (controlli di primo livello) all'interno dell'Unità Organizzativa;
- è supportato dai membri dell'Ufficio di staff in merito a pianificazione, esecuzione e monitoraggio controlli;
- interagisce con l'Autorità di Controllo in caso di eventuali controlli in merito al Modello volti a verificare l'effettiva osservanza del GDPR e altre disposizioni in materia di protezione dei dati personali

6 Modello operativo per la protezione dei dati personali

Le seguenti disposizioni interne e norme di autoregolamentazione hanno l'obiettivo di garantire la conformità ai requisiti del GDPR.

Ambito verticale	Artt. GDPR	Linee guida	Procedure
Accountability	5; 24	Main rules on accountability	/Il presente documento "Modello Generale per la protezione di Dati Personali"
Informative e consensi	6-14	Main rules on consent	Procedura "Gestione Informative e Consensi"
Diritti dell'interessato	12-23	Main rules on the right of data subjects, right to be forgotten and right to portability	Procedura "Gestione dei diritti degli interessati"
Data Protection by Design / Data Protection by Default	25	Main rules on privacy by design	Procedura di "Protezione dei dati fin dalla progettazione e per impostazione predefinita"
Fornitori e Contratti	28	Main rules on security	Procedura "Acquisti Non Merci[5]"(NDR - to be defined)
Registro dei trattamenti	30	Main rules on the record of processing activities	Procedura "Gestione registro dei trattamenti"

[5] Integrazione procedura già in essere

Rischi e Misure di sicurezza	32	Main rules on security	Procedura "Analisi dei rischi per gli interessati"
Data breach	33-34	Main rules on data breach	Procedura "gestione Data Breach"
Data Protection Impact Assessment e Consultazione Preventiva	35, 36	Main rules on data protection impact assessment	Procedura di "Valutazione di Impatto sulla Protezione dei Dati" (To be defined)
Trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali	44-50	Main rules on data transfers outside the UE	To be defined

Sono state inoltre recepite le linee guida condivise da Acoset S.p.A. SA in merito alle attività di profilazione (Main rules on profiling).

6.1 Accountability

Ai sensi dell'art. 5 del GDPR, il Titolare del trattamento non solo è tenuto a garantire il rispetto dei principi applicabili al trattamento di dati personali (ovvero i principi di "liceità, correttezza e trasparenza", "limitazione della finalità", "minimizzazione dei dati", "esattezza limitazione della conservazione" e "integrità e riservatezza"), ma il medesimo deve essere altresì "in grado di comprovarlo". Tale concetto è ulteriormente delineato nei suoi contorni dall'art. 24 dove viene stabilito che il Titolare del trattamento viene gravato dell'obbligo di mettere in atto (nonché di riesaminare e di aggiornare) misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Tali misure devono essere attuate dal Titolare del trattamento tenendo in considerazione tutta una serie di aspetti quali la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche e, ove ciò risulti proporzionato, le stesse devono includere l'attuazione di politiche adeguate in materia di protezione dei dati.

Acoset S.p.A., al fine di adeguarsi alle previsioni sopra riportate, ha definito un set di misure tecniche e organizzative, richiamate all'interno del presente documento, per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, tra le quali vi sono: la definizione di strutture, comitati e ruoli impegnati nella protezione dei dati personali; la nomina dei soggetti responsabili del trattamento dei dati personali; la formazione e l'istruzione del personale in materia di protezione dei dati personali; la creazione di procedure verticali e di strumenti operativi a supporto; la definizione di un sistema di controllo del modello di protezione dei dati personali.

6.2 Informative e consensi

Ai sensi degli artt. 6-14 del GDPR, il Titolare del trattamento è tenuto a rispettare una serie di condizioni volte ad assicurare la liceità del trattamento, quali ad esempio la raccolta del consenso esplicito dell'interessato per il trattamento dei propri dati personali per una o più specifiche finalità. Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il consenso al trattamento dei propri dati personali. In particolare, laddove l'interessato sia un minore la cui età è inferiore a 16 anni, il Titolare del trattamento è autorizzato a trattare i dati personali dello stesso soltanto se e nella misura in cui tale consenso è prestato o autorizzato dall'esercente la responsabilità genitoriale. Il Titolare del trattamento non può trattare categorie particolari di dati personali e/o dati relativi a condanne penali e reati, se non in presenza delle opportune condizioni quali ad esempio l'ottenimento del consenso esplicito da parte dell'interessato. Il GDPR, inoltre, impone al Titolare del trattamento di fornire all'interessato un set minimo di informazioni necessarie per garantire un trattamento corretto e trasparente. Le informazioni da fornire all'interessato variano in funzione delle modalità di raccolta dei dati personali: i dati personali, infatti, possono essere raccolti presso l'interessato o essere ottenuti attraverso canali alternativi (es. fonti pubbliche).

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

- dei modelli di informative e consensi che rispettano i requisiti del GDPR e derivano dal corretto censimento dei trattamenti effettuato nei registri dei trattamenti della società Acoset S.p.A.;
- un processo operativo per la gestione di informative e consensi, che si articola nelle fasi di Analisi del contesto, Identificazione delle condizioni da rispettare per il trattamento (es. raccolta del consenso esplicito), Somministrazione agli interessati dei documenti richiesti, Archiviazione della documentazione raccolta;
- uno strumento in cui raccogliere i modelli da adottare e la documentazione necessaria a dimostrare la liceità dei trattamenti effettuati dalla società Acoset S.p.A. (es. modulo di consenso firmato dall'interessato).

Si rimanda alla procedura "gestione informative e consensi" per la descrizione del processo operativo in tutte le sue componenti, ivi compresi presidi e attori coinvolti, nonché per i modelli utilizzati a supporto.

6.3 Diritti dell'interessato

Il GDPR introduce rilevanti novità riguardo i diritti dell'interessato e relative modalità d'esercizio degli stessi. Se da un lato il Regolamento rafforza diritti già presenti nel "Codice Privacy", dall'altro ne introduce di nuovi (diritto alla cancellazione e diritto alla portabilità). Ai sensi degli artt.15-23, infatti, gli interessati hanno il diritto di ottenere dal Titolare del trattamento: la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e in tal caso, di ottenere l'accesso ai dati personali; la rettifica dei dati personali inesatti che li riguardano senza ingiustificato ritardo; la cancellazione dei dati personali che li riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali in caso di una serie di motivi (es. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati); la limitazione del trattamento quando ricorre in caso di ipotesi specifiche (es. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali). Gli interessati, inoltre, hanno il diritto di: ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che li riguardano forniti a un Titolare del trattamento e hanno il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li hanno forniti; opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che li riguardano, compresa la profilazione sulla base di tali disposizioni; non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o che incida in modo analogo significativamente sulla propria persona.

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

- un processo operativo per la gestione dei diritti degli interessati, che si articola nelle fasi di Valutazione preliminare della richiesta, Evasione della richiesta e Archiviazione della richiesta;
- dei canali appositi per veicolare e raccogliere le richieste dagli interessati, quali ad esempio i siti web istituzionali della società Acoset S.p.A. in Italia (form ad hoc);
- uno strumento in cui tenere traccia delle richieste degli interessati gestita dalla società Acoset S.p.A. in Italia, ivi compresa la documentazione a supporto.

Si rimanda alla procedura "gestione dei diritti degli interessati" per la descrizione di ciascuna fase e dei relativi presidi, per l'individuazione degli attori coinvolti, nonché per il dettaglio degli strumenti utilizzati a supporto.

6.4 Data Protection by Design

Ai sensi degli art. 25, il Titolare del trattamento è tenuto a proteggere i dati personali fin dalla progettazione. Il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso.

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

- un processo operativo per la protezione dei dati personali fin dalla progettazione, che si articola nelle fasi di Analisi del contesto, Verifica conformità preliminare, Definizione e implementazione di un piano di interventi, Verifica conformità finale;
- una metodologia di lavoro e strumenti operativi volti a valutare, in fase di progettazione di qualsiasi progetto, servizio, sistema (sito web, software, soluzione IT, ambiente di lavoro, etc.), l'impatto in materia di protezione dei dati personali;
- uno strumento in cui raccogliere le valutazioni effettuate dalla società Acoset S.p.A. in Italia, ivi compresa la documentazione a supporto, opportunamente integrato con il portafoglio progetti in essere.

Nel futuro si procederà alla redazione della procedura "Protezione dei dati fin dalla progettazione e per impostazione predefinita" per la descrizione di ciascuna fase e dei relativi presidi, per l'individuazione degli attori coinvolti, nonché per il dettaglio della metodologia di analisi.

6.5 Data Protection by Default

Ai sensi degli art. 25, il Titolare del trattamento è tenuto a proteggere i dati personali per impostazione predefinita. Il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

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

- un elenco di misure tecniche e organizzative da adottare per impostazione predefinita, quali ad esempio:
  - l'analisi preliminare e l'individuazione, in sede di progettazione del trattamento, dei soli dati personali strettamente necessari per il perseguimento delle finalità definite;
  - delle configurazioni dei sistemi informativi e delle piattaforme di registrazione degli utenti che di default sono impostate al più alto livello di riservatezza e con le restrizioni più elevate, modificabili con espressa manifestazione di volontà degli utenti medesimi.
- uno strumento in cui raccogliere l'elenco delle misure tecniche e organizzative adottate per impostazione predefinita, in cui tenere traccia anche di tutte le modifiche effettuate.

Si rimanda al DPS (Documento Programmatico di Sicurezza) approvato dalla società.

6.6 Fornitori e Contratti

L'art. 28 del GDPR norma i casi in cui uno o più trattamenti debbano essere effettuati per conto del Titolare del trattamento, disciplinando quindi sotto il profilo della protezione dati personali l'eventualità che taluni trattamenti siano eseguiti da soggetti esterni (di seguito Responsabili del trattamento) per conto del Titolare. Il GDPR precisa i ruoli e le responsabilità in capo al Titolare e al Responsabile del trattamento, prevedendo anche che il Titolare ricorra unicamente a Responsabili del trattamento (ed eventuali sub-responsabili) che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della presente politica e garantisca la tutela dei diritti dell'interessato. Il GDPR, inoltre, prevede che i trattamenti effettuati da un Responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, 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.

6.7 Registro dei trattamenti

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).

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

- i registri dei trattamenti di dati personali della società Acoset S.p.A., sia in qualità di Titolare sia in qualità di Responsabile del Trattamento, conformi ai requisiti del GDPR;
- 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.

Si rimanda alla Procedura "Gestione del registro dei trattamenti" per la descrizione del processo operativo in tutte le sue componenti, ivi compresi presidi e attori coinvolti, nonché per i modelli di contratti utilizzati a supporto.

6.8 Rischi e Misure di sicurezza

Ai sensi dell'art. 32 del GDPR, il Titolare del trattamento e il Responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della

natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Le misure di tecniche e organizzative comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

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

- un processo operativo per valutare i rischi per i diritti e le libertà dell'interessato, articolato nelle fasi di Raccolta degli impatti, Valutazione delle probabilità, Calcolo del rischio, Definizione di un piano di trattamento, che comprende anche la definizione di misure di sicurezza volte a ridurre il rischio ad un livello ritenuto adeguato;
- una metodologia di lavoro e strumenti operativi volti a valutare i rischi per i diritti e le libertà dell'interessato, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- uno strumento in cui raccogliere le misure organizzative e tecniche adottate dalla società a fronte dei risultati delle valutazioni dei rischi per i diritti e le libertà dell'interessato, opportunamente collegato ai registri dei trattamenti della società Acoset S.p.A.

Si rimanda al DPS (Documento Programmatico di Sicurezza) approvato dalla società.

6.9 Data breach

Ai sensi degli artt. 33 e 34 del GDPR, in caso di *data breach*, il Titolare del trattamento è tenuto a notificare la violazione al Garante, senza ingiustificato ritardo e, se possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. L'obbligo non ricorre qualora il Titolare sia in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Il Titolare inoltre deve comunicare all'interessato

la violazione dei dati personali senza indebito ritardo in caso di rischio elevato per i diritti e le libertà delle persone fisiche.

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

- un processo operativo di Notifica/Comunicazione di un data breach, articolato nelle fasi di Segnalazione, Analisi, Valutazione, Decisione in merito alla notifica/comunicazione, Validazione e Invio della notifica/comunicazione, affidate ad organi/funzioni aziendali della società Acoset S.p.A.;
- una metodologia[6] di analisi del rischio per i diritti e le libertà dell'interessato associato al data breach oggetto di analisi e strumenti operativi volti a valutare, tra l'altro, la necessità di effettuare la Notifica al Garante/la Comunicazione agli interessati;
- uno strumento in cui raccogliere le violazioni di dati personali gestite dalla società Acoset S.p.A., ivi compresa la documentazione a supporto.

Si rimanda alla procedura "Gestione data breach" per la descrizione di ciascuna fase e dei relativi presidi, per l'individuazione degli attori coinvolti, nonché per il dettaglio della metodologia di analisi.

6.10 Data Protection Impact Assessment

Ai sensi dell'art. 35 del GDPR, il Titolare del trattamento è tenuto a effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti. In particolare, è prescritto di effettuare una DPIA qualora un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'effettuazione della DPIA non è obbligatoria[7] per ogni singolo trattamento ed è consentito effettuarne una complessiva per esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi (ad esempio per trattamenti che presentano analogie in termini di: natura, ambito, contesto, finalità, rischi). Ai sensi dell'art. 36, inoltre, il Titolare del trattamento è tenuto a consultare l'autorità di controllo - prima di procedere al trattamento - qualora la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

---

[6] Si precisa che la metodologia è conforme alle "Guidelines on Personal data breach notification under Regulation 2016/679" adottate il 3 ottobre 2017 (WP250)

[7] La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti: una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; il trattamento, su larga scala, di categorie particolari di dati personali, o di dati relativi a condanne penali e a reati; la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Acoset S.p.A., al fine di adeguarsi alle previsioni sopra riportate, procederà nel futuro ad adottare una procedura di "Valutazione di impatto sulla Protezione dei dati" per la descrizione di ciascuna fase e dei relativi presidi, per l'individuazione degli attori coinvolti, nonché per il dettaglio della metodologia di analisi.

6.11 Trasferimento dati verso Paesi terzi o organizzazioni internazionali

Ai sensi degli articoli di cui al Capo V del GDPR (artt. 44-50), il Titolare del trattamento e il Responsabile del trattamento sono tenuti, in caso di trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali, ad assicurare agli interessati il medesimo livello di protezione di cui godrebbero se i dati venissero trattati all'interno dell'UE. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. La decisione di adeguatezza, tuttavia, non è l'unico strumento in virtu' del quale un trasferimento può avvenire. Infatti l'art. 46, comma 1, del GDPR specifica che «in mancanza di una decisione ai sensi dell'articolo 45, comma 3, il Titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate[8] e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi». In mancanza di una decisione di adeguatezza ex art. 45.3 o di garanzie adeguate ex art. 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti se si verificano delle condizioni particolari (es. l'interessato acconsente esplicitamente al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato).

Acoset S.p.A., non gestisce trasferimenti di dati verso Paesi terzi o organizzazioni Internazionali.

---

[8] Possono costituire garanzie adeguate senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; le norme vincolanti d'impresa; le clausole tipo di protezione dei dati adottate dalla Commissione; un codice di condotta; un meccanismo di certificazione

7 Modello architetturale per la protezione dei dati personali

Viene adottato un modello architetturale per la protezione dei dati personale al fine di garantire un livello di sicurezza adeguato al rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

7.1 Dati personali

Il GDPR richiede al Titolare del trattamento di classificare opportunamente le categorie di dati personali trattati, con particolare riferimento a dati appartenenti a "categorie particolari di dati" [9] e "dati relativi a condanne penali e reati". Ai sensi degli artt. 9-10 del GDPR, infatti, il Titolare del trattamento è tenuto a trattare tali dati solo a fronte del rispetto di determinate condizioni, quali ad esempio la raccolta del consenso esplicito da parte dell'interessato per una o più finalità specifiche legate al trattamento o il caso in cui il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali. il Titolare del trattamento, inoltre, è tenuto a condividere con l'interessato:

- ai sensi degli artt. 13-14 del GDPR, il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ai sensi dell'art. 20 del GDPR, i dati personali soggetti a portabilità. Il GDPR, infatti, consente all'interessato di ricevere i dati personali forniti a un Titolare «in un formato strutturato, di uso comune e leggibile da un dispositivo automatico», e trasmetterli a un altro Titolare del trattamento «senza impedimenti».

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

- una classificazione dei dati personali allineata alle categorie di dati personali sopra indicate, individuando e tenendo traccia anche dei dati personali soggetti a portabilità;
- i periodi di conservazione dei dati personali trattati dalla società Acoset S.p.A., conformi agli obblighi di legge (ove presenti), oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

---

[9] dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

7.2 Sistemi informativi

La Società dispone dell'elenco degli applicativi, integrato nel catalogo degli applicativi aziendali, che trattano dati personali di cui la società Acoset S.p.A. è titolare o responsabile del trattamento. Nello specifico, grazie alle informazioni contenute all'interno del registro dei trattamenti, la Società dispone delle seguenti informazioni per ciascun applicativo che tratta dati personali: processi e attività ("contenitori" del trattamento), finalità del trattamento, categorie di dati trattati, categorie di interessati dal trattamento, referenti interni per la protezione dei dati personali, categorie di soggetti autorizzati al trattamento, responsabili esterni del trattamento, eventuali comunicazioni e trasferimenti dati extra UE.

Acoset S.p.A., inoltre, dispone delle informazioni in merito alle infrastrutture (es. Building; Server) presso le quali risiedono tali dati, sia proprietarie sia di Soggetti terzi. In particolare, la Società presta attenzione a eventuali casi in cui i dati personali sono archiviati o trattati al di fuori dei confini europei, adottando le opportune garanzie in funzione del Paese di riferimento per assicurare un livello adeguato di protezione dei dati personali trasferiti.

7.3 Misure di sicurezza

Ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il Responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

La Società, alla luce delle indicazioni emerse dalla valutazione dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche connessi ai trattamenti censiti nel registro dei trattamenti, ha individuato alcune misure di sicurezza volte a mitigare adeguatamente il rischio. La Società inoltre, adotta un sistema di gestione della Sicurezza che prevede il controllo e il miglioramento continuo dei processi e dei prodotti, valutando periodicamente l'efficacia delle misure implementate, mediante attività di assessment che insistono su "organizzazione e ruoli", "persone, cultura e competenze", "processi e regole", "documentazione", "tecnologie e strumenti", così come definito nel "Modello di controllo per la protezione dei dati personali". La Società ha quindi individuato ulteriori misure di sicurezza, volte a mitigare ulteriormente il rischio, a maggior tutela di Acoset S.p.A. e degli interessati.

Si rimanda al "Documento programmatico per la sicurezza dei dati" e ai suoi allegati per la descrizione di dettaglio

8 Modello di controllo per la protezione dei dati personali

Viene adottato un sistema di controllo della protezione dei dati personali, integrato nel "sistema aziendale dei controlli interni", al fine di garantire il rispetto delle prescrizioni del GDPR e, in particolare, l'adeguatezza delle procedure, dei processi, delle politiche e dell'organizzazione interna con il fine di prevenire rischi di "non conformità"[10].

Il sistema di controllo della protezione dei dati personali adottato prevede le seguenti componenti:

- monitoraggio degli aggiornamenti normativi in materia di protezione dei dati personali, con particolare riferimento alle implicazioni dal punto di vista delle sanzioni legate al mancato rispetto delle prescrizioni delle normative;
- *"risk assessment"*, ovvero individuazione e valutazione dei rischi potenziali, individuazione e valutazione dei presidi di conformità, determinazione del rischio residuo o inerente, eventuale formulazione di proposte di intervento e successivo monitoraggio;
- *"testing"*, ovvero verifiche di funzionamento relative al grado di aderenza delle tematiche controllate al GDPR e alle altre norme in materia di protezione dei dati personali, anche attraverso il supporto di un cruscotto di KPI;
- *"reporting"*, ovvero condivisione informazioni agli organi sociali e a determinate strutture aziendali sull'esito delle attività svolte e sugli eventuali interventi di miglioramento ritenuti necessari in materia di protezione dei dati personali;
- consulenza a strutture e ruoli aziendali (es. Referenti Data Protection) relativamente a tematiche connesse alla protezione dei dati personali in cui assume rilievo il rischio di non conformità;
- formazione, ovvero supporto al servizio "personale" nell'individuazione di iniziative formative attinenti a tematiche in cui assume rilievo il rischio di non conformità in materia di protezione dei dati personali.

[10] Rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative e di autoregolamentazione

9 Appendice

9.1 Normative e linee guida

Di seguito si riportano l'elenco di normative e linee guida in materia di protezione dei dati personali in vigore alla data di predisposizione del presente documento:

- **Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio** del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- **Decreto Legislativo 30 giugno 2003, n.196** (in Suppl. ordinario n. 123 alla Gazz. Uff., 29 luglio, n. 174). - Codice in materia di protezione dei dati personali (Codice Privacy);
- **Legge di Delegazione** n. 163, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017";
- **Linee guida del Gruppo di Lavoro istituito ai sensi dell'art. 29 della direttiva 95/46** (c.d. WP29):
  - "Guidelines on the right to data portability" adottate il 5 aprile 2017 (WP242 rev.01);
  - "Guidelines on Data Protection Officers ('DPOs')", adottate il 5 aprile 2017 (WP243 rev.01);
  - "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", adottate il 4 aprile 2017 (WP248);
  - "Guidelines on Personal data breach notification under Regulation 2016/679", adottate il 3 ottobre 2017 (WP250);
  - "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", adottate il 3 ottobre 2017 (WP251);
  - "Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679", adottate il 3 ottobre 2017 (WP253);
  - "Guidelines on Consent under Regulation 2016/679", adottate il 28 novembre 2017 (WP259);
  - "Guidelines on transparency under Regulation 2016/679" (WP260).

9.2 Documenti richiamati

Di seguito si riporta l'elenco dei documenti richiamati nel presente Modello Generale, utili per approfondire le valutazioni alla base delle scelte effettuate:

- Modello **organizzativo** per la protezione dei dati personali
- Modello **operativo** per la protezione dei dati personali (rappresentato dalle procedure per la protezione dei dati personali)
- Modello **architetturale** per la protezione dei dati personali
- Modello di **controllo** per la protezione dei dati personali.
- Documento programmatico per la sicurezza (DPS) adottato da Acoset nel 2017.