Linee Guida Privacy

Solesi S.p.A.

[*v. 2022-02*]

Rev.	Data	Sommario delle modifiche	Approvazione
0	01/02/2022	Adozione ex art. 30, par. 1 del GDPR	

1 Premessa

Obiettivi e contenuti

Le presenti **Linee Guida** sono adottate da Solesi S.p.A. (di seguito la "Società" o il "Titolare").

Il presente documento è adottato allo scopo di definire ruoli, responsabilità e principi di comportamento applicabili a tutte le attività di trattamento dei dati personali svolte sotto l'autorità della Società, nonché di fornire le linee guida in base a cui dovranno essere adottate le procedure e i regolamenti aziendali che disciplinano attività rilevanti ai fini *privacy*.

Norme di riferimento

Le Linee Guida sono adottate ai fini della *compliance* alle previsioni delle seguenti fonti:

- 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) (nel seguito, il "**Regolamento**" o "**GDPR**");
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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", come da ultimo modificato dal Decreto Legislativo 10 agosto 2018, n. 101, pubblicato in G.U. n. 205 del 4 settembre 2018 (nel seguito, "**Codice Privacy**");
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)
- Linee guida, Raccomandazioni, Opinioni e altri documenti pubblicati dallo *European Data Protecion Board* ("**EDPB**") istituito dall'art. 68 del GDPR, che ha sostituito il Gruppo di lavoro *ex* art. 29 della Direttiva 95/46/CE;
- Linee guida e Provvedimenti emanati dal Garante per la protezione dei dati personali ("**Garante Privacy**").

Ambito di applicazione

Le presenti Linee Guida si applicano a:

- tutti i trattamenti di dati personali effettuati dalla Società direttamente o indirettamente tramite terzi fornitori di servizi;
- tutte le attività di trattamento eventualmente svolte dalla Società per conto terzi (anche nell'ambito del Gruppo di appartenenza.

Non rientrano nell'ambito di applicazione del presente documento:

- i trattamenti di dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto;
- i trattamenti di dati personali effettuati da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico, senza alcuna connessione con attività commerciali o professionali;
- i trattamenti riferiti ad informazioni anonime, ossia informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

In particolare, sono **"Destinatari"** delle previsioni delle presenti Linee Guida, per quanto di competenza in base alle mansioni/incarichi assegnati, tutto il personale impiegato presso le unità organizzative della Società coinvolte nei processi di trattamento.

Pubblicazione delle Linee Guida e della documentazione rilevante

Il presente documento è messo a disposizione di tutti i Destinatari e pubblicato sulla rete aziendale.

Il Titolare, altresì, mette a disposizione dei Destinatari, con la medesima modalità sopra indicata, la ulteriore documentazione di interesse nell'ambito del sistema di gestione dei dati personali dallo stesso implementato; il Titolare valuta, altresì, l'opportunità di definire specifiche regole per l'accesso e la modifica della suddetta documentazione in relazione al ruolo e alle mansioni affidate.

2 Principi applicabili al trattamento di dati personali

Tutte le operazioni di trattamento di dati personali svolte sotto l'autorità della Società devono conformarsi ai seguenti principi, nel rispetto delle previsioni di cui all'art. 5 del GDPR.

liceità

- il trattamento è lecito solo se fondato su uno dei presupposti tassativamente individuati dal GDPR o dalla normativa nazionale rilevante:
  - consenso al trattamento dei dati personali espresso dall'interessato;
  - esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dell'interessato medesimo;
  - adempimento di un obbligo legale applicabile al titolare del trattamento;
  - salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
  - esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
  - perseguimento del legittimo interesse del titolare del trattamento o di terzi[1], a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
- per ciascun trattamento è individuata la relativa base legale, debitamente censita all'interno del Registro dei trattamenti adottato dal Titolare ai sensi dell'art. 30 del GDPR.

trasparenza e correttezza

- i dati sono trattati per finalità determinate, esplicite e legittime;
- all'interessato sono esplicitamente comunicate le modalità con cui i dati personali sono raccolti, utilizzati, consultati o altrimenti trattati;
- le comunicazioni relative al trattamento di tali dati personali sono facilmente accessibili e comprensibili e, a tal fine, viene utilizzato un linguaggio semplice e chiaro.

limitazione della finalità

I dati, raccolti per finalità determinate, esplicite e legittime, sono successivamente trattati in modo che non vi sia incompatibilità con tali finalità.

Laddove si determini l'esigenza di introdurre una nuova finalità per un dato trattamento – incompatibile con le finalità per cui i dati personali sono stati inizialmente raccolti – è necessario sottoporre tempestivamente agli interessati la documentazione aggiornata (i.e. informativa e, ove applicabile, consenso).

Ai fini della verifica della compatibilità della nuova finalità con quella per cui i dati personali sono stati raccolti inizialmente, si tiene conto di:

- ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- il contesto in cui i dati personali sono stati raccolti, con particolare riferimento alla relazione tra l'interessato e il Titolare;
- la natura dei dati personali (con particolare riferimento al trattamento di categorie particolari di dati personali *ex* art. 9 del GDPR e/o di dati relativi a condanne penali e a reati *ex* art. 10 del GDPR;
- le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- l'esistenza di garanzie adeguate (ad es. la cifratura o la pseudonimizzazione).

[1] Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi o relativi al traffico di rete per la gestione della sicurezza delle reti stesse e delle informazioni.

minimizzazione

- i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- se non è possibile utilizzare dati anonimi o aggregati, non riconducibili a soggetti identificati od identificabili, non sono impiegati dati personali eccedenti quelli necessari;
- sono adottate idonee misure affinché i dati personali dell'interessato non siano resi accessibili ad un numero indefinito di persone fisiche, senza l'intervento della persona fisica.

esattezza

- i dati personali oggetto di trattamento sono esatti;
- i dati personali sono oggetto di aggiornamento ogni qualvolta si renda necessario

limitazione della conservazione

- i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati;
- i dati personali possono essere conservati per periodi più lunghi a condizione che gli stessi siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, par. 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate adottate a tutela dei diritti e delle libertà dell'interessato;
- se i dati personali in possesso del Titolare non consentono di identificare una persona fisica (ad esempio, a seguito della cancellazione/anonimizzazione di dati personali in applicazione delle politiche di *data retention*), lo stesso non è tenuto a conservare, acquisire o trattare ulteriori informazioni al solo fine di identificare l'interessato per ottemperare alle previsioni del GDPR (ad es., in caso di esercizio da parte dell'interessato dei diritti previsti dagli artt. da 15 a 20 del GDPR); ad ogni modo, ai fini dell'esercizio dei diritti da parte dell'interessato, il Titolare si avvale di tutte le informazioni aggiuntive eventualmente fornite a tal fine dall'interessato stesso. Il Titolare informa l'interessato nei casi in cui possa dimostrare di non essere in grado di identificarlo.

integrità e riservatezza

- i dati personali sono trattati in modo da garantirne l'integrità e la riservatezza, impedendo l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate.

accountability

- il Titolare implementa misure tecniche e organizzative adeguate a garantire e dimostrare che il trattamento dei dati personali è effettuato nel rispetto delle previsioni del GDPR.

Come meglio disciplinato nel seguito del presente documento, ai fini del rispetto dei principi sopra sintetizzati, la Società:

- definisce ed implementa misure tecniche e organizzative adeguate al fine di garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- cura il processo di responsabilizzazione di tutti i soggetti coinvolti nel trattamento dei dati, mediante il conferimento e l'aggiornamento delle nomine e delle istruzioni necessarie a garantire il rispetto della normativa vigente e dei relativi principi;
- garantisce che i dati oggetto di trattamento siano messi a disposizione e acceduti esclusivamente dalle funzioni e dai soggetti che ne abbiano la necessità in virtù delle mansioni e degli incarichi affidati;
- definisce ed implementa misure tecniche e organizzative atte a garantire un adeguato livello di protezione da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali; in particolare, sono

previste misure operative per la gestione della creazione e disabilitazione delle utenze, nonché appropriate misure di sicurezza per la gestione delle credenziali d'accesso ai sistemi informatici;

- istituisce e mantiene aggiornato il Registro dei trattamenti di cui all'art. 30 del GDPR. In particolare, il Registro dei trattamenti indica il periodo di conservazione dei dati associato a ciascun trattamento al fine di individuare eventuali casistiche in cui sia necessario procedere alla cancellazione dei dati;
- provvede tempestivamente a comunicare agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro le necessarie informazioni attraverso degli appositi moduli di informativa e richiesta del consenso in ottemperanza ai requisiti previsti dagli artt. 7, 8, 13 e 14 del GDPR;
- inserisce all'interno dei moduli di informativa un riferimento alle tempistiche di conservazione dei dati, nonché alle modalità con cui gli interessati possono richiederne la cancellazione;
- a seguito di eventuali inserimenti e/o modifiche ai trattamenti aggiorna tempestivamente il Registro *ex* art. 30 del GDPR e i connessi moduli di informativa e/o consenso.
- qualora intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, fornisce preventivamente all'interessato il modulo di informativa aggiornato;
- garantisce il tempestivo riscontro alle richieste degli interessati in relazione all'esercizio dei diritti loro riconosciuti in forza della normativa di riferimento. Tali diritti sono esplicitamente indicati nelle informative fornite agli interessati.

Privacy by design & by default

L'art. 25 del GDPR introduce i concetti di *privacy by design* e di *privacy by default*:

- con l'espressione "*privacy by design*" si intende la necessità di considerare gli aspetti di privacy nelle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento, al fine di attuare in modo più efficace i principi di protezione dei dati. In particolare, il GDPR prevede, con riferimento a tale principio, che, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento ha il dovere di mettere in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati;
- con l'espressione "*privacy by default*" si intende il principio tale per cui devono essere trattati solo i dati personali necessari per ogni specifica attività di trattamento.

Al fine di poter dimostrare la conformità ai requisiti previsti dal GDPR, si prevede l'avvio di un processo di analisi dei rischi e degli impatti privacy (c.d. *Privacy Impact Assessment – PIA*) in connessione alle fasi di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti che implicano il trattamento di dati personali (cfr. par. 10).

Inoltre, la Società mette in atto misure tecniche e organizzative adeguate a 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.

3 Organigramma Privacy: ruoli e responsabilità

Ai fini della compliance alla normativa vigente in materia di privacy e sue evoluzioni, la Società ha definito il proprio organigramma/modello organizzativo in materia privacy, identificando i ruoli e le figure organizzative, in coerenza con i presidi di controllo richiesti.

Titolare del trattamento

Il GDPR (art. 4, par. 1, n. 7)) definisce "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; 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.

Nell'ambito del contesto organizzativo, il "Titolare" del trattamento è pertanto da individuare nella Società, che opera per il tramite del legale rappresentante.

A tal fine, la Società:

- determina le finalità e i mezzi del trattamento;
- cura il processo di responsabilizzazione di tutti i soggetti coinvolti nel trattamento dei dati (*accountability*), mediante il conferimento e l'aggiornamento delle nomine e delle istruzioni necessarie a garantire il rispetto della normativa vigente e dei relativi principi;
- garantisce che i responsabili del trattamento adottino misure tecniche e organizzative adeguate, tramite la formalizzazione di nomine *ad hoc*, nonché l'eventuale svolgimento di apposite verifiche e *audit* periodici;
- garantisce il rispetto dei principi di liceità, correttezza, minimizzazione, limitazione della finalità del trattamento e della conservazione dei dati, anche tramite strumenti tecnici adeguati, secondo l'evoluzione tecnologica (*privacy by design e by default*);
- garantisce la sicurezza, la correttezza e l'aggiornamento dei dati trattati, anche mediante l'istituzione e la tenuta del Registro dei trattamenti;
- valuta periodicamente il rischio dei trattamenti svolti e, quando necessario, effettua, anche con il supporto di consulenti esterni, la valutazione di impatto privacy (DPIA - *Data Protection Impact Assessment*) e la consultazione preliminare al Garante Privacy;
- garantisce che le misure di sicurezza adottate nell'ambito della realtà aziendale siano adeguate, anche in relazione all'evoluzione tecnologica dei sistemi informativi;
- all'interno del contesto aziendale, eroga adeguata formazione a tutto il personale e ai collaboratori coinvolti nelle attività di trattamento dei dati personali.

Secondo quanto previsto dall'art. 24 del GDPR, il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento venga effettuato conformemente al Regolamento (principio di "*accountability*").

Tali misure:

- vanno valutate tenendo in considerazione una serie di elementi, tra cui 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;
- devono essere riesaminate e aggiornate, qualora necessario;
- includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del Titolare del trattamento, se ciò è proporzionato rispetto alle attività di trattamento.

Gli artt. 40 e 42 specificano, inoltre, che il Titolare può dimostrare la conformità del trattamento dei dati al GDPR anche attraverso l'adozione delle misure di sicurezza o l'adesione ai codici di condotta o un meccanismo di certificazione.

Nell'ambito dello svolgimento delle proprie attività, le Società operano anche in qualità di Responsabile ai sensi dell'art. 28 del Regolamento, quando coinvolte nel trattamento di dati personali la cui titolarità spetta ad un altro soggetto. In tali circostanze, queste operano in base alle istruzioni fornite dal singolo titolare del trattamento. Sul punto, si rinvia al par. 3.6.2.

Contitolari del trattamento

Il GDPR (art. 26) stabilisce che una situazione di "contitolarità" si configura laddove due o più titolari del trattamento definiscano congiuntamente le finalità e i mezzi del trattamento; le rispettive responsabilità sono disciplinate mediante un accordo interno. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato, che può comunque esercitare i propri diritti ai sensi del Regolamento nei confronti di e contro ciascun titolare del trattamento.

Eventuali situazioni di contitolarità sono evidenziate nel Registro dei trattamenti istituito e aggiornato dalla Società.

In caso di trattamenti di dati personali in situazione di contitolarità è cura di ciascuna funzione responsabile, nella fase di aggiornamento del Registro dei trattamenti (cfr. par. 8), tenere conto dell'eventuale coinvolgimento di ulteriori soggetti con ruolo di co-titolari.

Responsabile per la protezione dei dati personali

Il GDPR (art. 37) prevede che il Titolare e il Responsabile del trattamento individuino un Responsabile della protezione dei dati/Data Protection Officer ("DPO"), nominando una figura professionale interna o esterna alla Società, dotata di adeguate competenze in campo giuridico e informatico, nonché in materia di valutazione del rischio e di analisi dei processi. Il GDPR individua i casi tassativi di nomina del DPO e definisce, unitamente alle Linee guida e ad altri documenti rilevanti pubblicati dalle Autorità garanti, i compiti e le mansioni di competenza dello stesso.

In particolare, ai sensi dell'art. 37, par. 1 del GDPR la nomina del DPO è obbligatoria nei casi in cui:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti:
  - che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
  - su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e reati.

Inoltre, l'art. 37, par. 2 del GDPR prevede che un medesimo gruppo imprenditoriale possa nominare un unico DPO, a condizione che lo stesso sia raggiungibile da ogni "stabilimento".

In ottemperanza ai requisiti previsti dall'art. 39 del GDPR e dalle linee guida emesse dal WP29 e/o dalla EDPB sull'argomento, al DPO sono attribuiti i seguenti compiti:

- informare e fornire consulenza ai soggetti coinvolti nel trattamento dei dati personali in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati;
- vigilare sull'osservanza della normativa nazionale e sovranazionale relativa alla protezione dei dati, dei provvedimenti delle Autorità, nonché delle disposizioni contenute negli atti e documenti aziendali;
- curare la tenuta del Registro delle attività di trattamento, monitorandone l'attualità e il tempestivo aggiornamento, con il supporto delle funzioni di volta in volta coinvolte;
- presidiare i processi di valutazione d'impatto sulla protezione dei dati (DPIA), esprimendo un parere motivato sulla necessità/opportunità di condurre o meno la DPIA, sulla metodologia da adottare e sulle salvaguardie da applicare (comprese le misure tecniche ed organizzative atte ad attenuare i rischi per i diritti e gli interessi degli interessati), nonché sorvegliarne lo svolgimento;
- cooperare con l'Autorità garante e fungere da punto di contatto per la stessa, per questioni connesse al trattamento;

- intervenire nelle iniziative e nei piani di formazione finalizzati alla diffusione della cultura aziendale in materia di trattamento dei dati e alla condivisione delle Linee Guida.

In considerazione delle attività di trattamento svolte in qualità di Titolare del trattamento non ricorrono in capo alla Società i presupposti per la nomina obbligatoria del DPO. In particolare, non si ritiene che sia soddisfatto il requisito della "larga scala", così come definito sia dal GDPR (Considerando 91) che dalle Linee guida del WP29 in materia di nomina del DPO.

Amministratori di sistema

La figura dell'amministratore di sistema è definita dal provvedimento del Garante privacy del 27 novembre 2008 (recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*"), così come successivamente modificato dallo stesso Garante con provvedimento del 25 giugno 2009.

In particolare, il Garante individua gli amministratori di sistema in quelle figure professionali incaricate della gestione e manutenzione di impianti di elaborazione o di sue componenti, nonché nelle altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi.

In ottemperanza al citato provvedimento, ciascun Titolare/Responsabile di trattamenti effettuati con strumenti elettronici è tenuto ad adottare specifiche misure e accorgimenti con riferimento agli amministratori di sistema:

- l'attribuzione delle funzioni di amministratore di sistema deve avvenire, mediante specifica nomina, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- gli estremi identificativi delle persone fisiche Amministratori di Sistema, unitamente all'elenco degli ambiti di operatività agli stessi consentiti per i trattamenti di dati personali di cui la Società è titolare, come previsto al punto 2, lettera c) del Provvedimento del Garante del 27 novembre 2008 e s.m.i., devono essere riportati in un documento interno da mantenere aggiornato e disponibile al personale, nonché in caso di accertamenti da parte del Garante;
- devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema tramite opportuni "*access log*"[2];
- l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare (o del Responsabile) del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;

Nel caso in cui la Società affidi le attività di supporto e manutenzione in ambito *information technology* in *outsourcing* ad un fornitore esterno, ai sensi dell'art. 28 del GDPR e del citato Provvedimento del Garante del 27 novembre 2008 e s.m.i., nomina il fornitore quale amministratore di sistema, nonché responsabile del trattamento. In tal caso, il fornitore esterno si impegna, tra le altre cose, a:

- documentare e conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema e a metterle a disposizione del Titolare, in base a specifica richiesta;

[2] Per "access log" si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

- verificare, su base almeno annuale, l'operato delle persone fisiche identificate quali amministratori di sistema nell'ambito delle attività affidate in outsourcing dal Titolare, al fine di monitorarne la rispondenza alle misure organizzative, tecniche e di sicurezza previste.

Gli "*access log*" devono avere le seguenti caratteristiche:

- comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
- essere completi, ossia devono comprendere tutti gli eventi di accesso interattivo che interessino gli Amministratori di Sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali;
- essere inalterabili;
- essere tali da rendere possibile una verifica della loro integrità al raggiungimento dello scopo per cui sono richiesti.

Nel caso in cui l'Amministratore sia trasferito ad una struttura aziendale diversa da quella iniziale, è necessario aggiornare la nomina al fine di indicare correttamente le attività di competenza ed i correlati trattamenti di dati personali.

La designazione può essere revocata come segue:

- revoca espressa: effettuata nel caso in cui, con riferimento alla nuova posizione, non sussistano i requisiti per la nomina;
- revoca tacita: interviene automaticamente in caso di cessazione del rapporto di lavoro.

L'elenco delle persone fisiche nominate Amministratori di Sistema dalla Società, in connessione alla funzione/struttura di appartenenza è reso disponibile nella cartella dedicata sulla rete aziendale (cfr. precedente par. 1.4).

Struttura organizzativa aziendale

Tutte le funzioni aziendali sono responsabili della corretta gestione dei dati personali trattati e del rispetto delle disposizioni della Società, compreso quanto definito nelle presenti Linee Guida.

A tal fine, le funzioni aziendali si adeguano alle istruzioni impartite dal Titolare, tramite la normativa interna e le eventuali lettere di autorizzazione al trattamento di dati personali; in particolare, il GDPR prevede che il Titolare provveda ad autorizzare le persone preposte ad effettuare un trattamento di dati personali sotto la propria autorità.

Nell'ambito della propria struttura organizzativa, Solesi individua e autorizza formalmente i soggetti – dipendenti e collaboratori – cui sono demandate le attività connesse al trattamento di dati personali di competenza della funzione di riferimento (c.d. genericamente "Incaricati del trattamento", cfr. par. 3.5.2).

Ai fini dell'adeguata responsabilizzazione di tutti i soggetti coinvolti, laddove ritenuto opportuno, la Società individua espressamente coloro che hanno una particolare capacità di incidere sulle modalità di trattamento dei dati personali nell'ambito dell'unità organizzativa di riferimento, in virtù delle funzioni di responsabilità rivestite e delle specifiche mansioni svolte ("Responsabili di funzione").

Mediante il processo di responsabilizzazione dei Responsabili di funzione, il Titolare del trattamento dei dati si pone l'obiettivo di semplificare l'organizzazione privacy interna e garantire una più efficiente ed efficace possibilità di rispondere agli obblighi di *accountability* imposti dal GDPR.

3.1.1 Responsabili di funzione

I Responsabili di funzione, in qualità di soggetti/incaricati autorizzati al trattamento da parte del Titolare, svolgono i seguenti compiti:

- mantenere un censimento aggiornato delle operazioni di trattamento che rientrano nel proprio ambito di competenza, anche ai fini dell'adeguamento del Registro dei trattamenti (cfr. par. 8);

- monitorare la coerenza e l'attualità delle istruzioni fornite ai propri collaboratori con le mansioni a questi assegnate, in particolare con riferimento ai casi di cambio mansioni e/o sviluppo di nuove attività;
- assicurare la corrispondenza tra gli ambiti operativi dei propri collaboratori e le autorizzazioni di accesso a dati e sistemi agli stessi conferite;
- verificare che i propri collaboratori partecipino alle iniziative formative loro dedicate;
- coordinarsi con la Funzione Legal, al fine di assicurare che siano correttamente disciplinati, sotto il profilo della tutela dei dati, i rapporti con i terzi incaricati di effettuare, per conto del Titolare, attività strumentali che comportano il trattamento di dati personali di pertinenza della funzione di riferimento;
- monitorare l'effettiva esecuzione delle misure di sicurezza, anche nei riguardi delle terze parti con cui lo stesso si rapporta;
- informare il Titolare e la Funzione IT su eventuali violazioni di dati personali e su qualsiasi situazione di non conformità, attuale o presunta, dei trattamenti inclusi nell'ambito di sua competenza alle disposizioni di legge e delle presenti Linee Guida.

Nello svolgimento dei loro compiti, i Responsabili di funzione garantiscono al Titolare il pieno accesso ai documenti e alle informazioni rilevanti in relazione ai trattamenti di dati personali da loro effettuati, ai fini della valutazione periodica dei livelli di rischio afferenti le attività di trattamento e nella collaborazione con le Autorità competenti.

3.1.2 Incaricati del trattamento

La Società, in qualità di Titolare per i trattamenti di competenza, autorizza formalmente tutti i soggetti persone fisiche (i.e. dipendenti a tempo indeterminato o determinato, lavoratori "somministrati", lavoratori a progetto, stagisti, collaboratori ecc.) che, agendo sotto la propria autorità, effettuano un trattamento di dati personali o vi hanno accesso ("Incaricati").

La suddetta autorizzazione include, altresì, le istruzioni cui l'Incaricato deve attenersi scrupolosamente nello svolgimento delle attività inerenti il trattamento di dati personali.

A tale scopo, la Società provvede a consegnare al neoassunto/dipendente (se applicabile) la lettera di autorizzazione al trattamento dei dati personali, in base alla specifica mansione assegnata.

Ciascun Responsabile di funzione:

- conserva una lista degli Incaricati, autorizzati al trattamento dei dati nell'ambito della propria funzione, in cui indicare, tra l'altro, l'ambito del trattamento e le tipologie di dati personali corrispondenti a ciascuno, anche mediante aggregazione per aree omogenee di incarico;
- mantiene ed aggiorna i modelli di nomina predisposti, al fine di garantire la coerenza con le attività effettivamente svolte dall'Incaricato.

In relazione alle attività svolte nell'ambito della struttura organizzativa gli Incaricati del trattamento sono tenuti a:

- svolgere le attività previste per i trattamenti secondo le istruzioni ricevute per iscritto dal Titolare;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Titolare;
- rispettare le norme di sicurezza per la protezione dei dati;
- informare il proprio Responsabile di funzione e la Funzione IT in caso di violazione dei dati personali, accertata o presunta.

3.1.3 Formazione e sensibilizzazione

La Società si assicura che chiunque agisca sotto la propria autorità non tratti dati personali se non è stato istruito in tal senso.

A tal fine, viene definito anche un piano di formazione e informazione finalizzato alla sensibilizzazione del

personale aziendale circa la necessità di attenersi alle disposizioni in materia di trattamento dei dati personali, che prevede:

- attività di formazione periodica specifica rivolta al personale coinvolto nelle attività di trattamento, nonché sessioni formative ad hoc per i neo-assunti;
- corsi focalizzati su specifici Provvedimenti dell'autorità rilevanti nell'ambito delle attività svolte dal Titolare.

Responsabile del trattamento

Il GDPR (art. 4, par. 1, n. 8)) definisce "Responsabile del trattamento" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare del trattamento.

L'art. 28, par. 2, del GDPR prevede che il Responsabile del trattamento possa ricorrere ad un altro responsabile (Sub-Responsabile), previa autorizzazione – generale o specifica – del titolare del trattamento.

Solesi nomina Responsabili del trattamento quei fornitori/società (anche del medesimo Gruppo) e più in generale le terze parti che trattano i propri dati personali per loro conto e/o vi hanno accesso; si tratta, in dettaglio, di soggetti esterni alla realtà aziendale e possono essere persone fisiche o società – anche facenti parte del medesimo Gruppo – enti, associazioni o organismi cui il Titolare affida compiti di gestione e controllo del trattamento dei dati personali mediante atto formale.

La nomina del fornitore a Responsabile del trattamento viene formalizzata dalla Società nell'ambito del contratto sottoscritto con lo stesso o con atto separato; attraverso detta nomina, la Società fornisce al Responsabile precise istruzioni in merito alle modalità di trattamento dei dati personali.

In conformità alle previsioni del GDPR, con l'atto di nomina il Titolare impone al Responsabile, tra l'altro, di:

- trattare i dati personali soltanto in base ad istruzioni documentate, anche in caso di trasferimento di dati personali verso un Paese fuori dall'UE o un'organizzazione internazionale e fatte salve le deroghe previste dal medesimo GDPR (i.e. trasferimento verso Paesi extra-UE in base a specifici obblighi giuridici);
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza indicate all'art. 32 del GDPR;
- rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del GDPR in caso di ricorso a un altro Responsabile del trattamento;
- tenendo conto della natura del trattamento, supportare il Titolare stesso con misure tecniche e organizzative adeguate ai fini dell'adempimento degli obblighi inerenti i casi di esercizio dei diritti dell'interessato di cui al Capo III del GDPR;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
- su indicazione del Titolare, cancellare e/o restituire tutti i dati personali in suo possesso al termine della prestazione di servizi che implica il trattamento di dati del Titolare, fatte salve le deroghe previste dal medesimo GDPR (i.e. conservazione dei dati oggetto della prestazione, prevista dalla legge);
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti sia nell'atto di nomina che nel GDPR, nonché consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi appositamente incaricato;
- informare immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi le previsioni del GDPR o di altre disposizioni di legge, nazionali o sovranazionali, in materia di protezione dei dati.

La Società ha predisposto un modello di contratto ai sensi dell'art. 28 GDPR tra il Titolare e il Responsabile del trattamento.

3.1.4 Gestione delle terze parti

Il processo di identificazione dei casi in cui si rende necessario ricorrere ad una terza parte per la gestione di tutto o parte del trattamento, si struttura nelle seguenti fasi:

1. nell'ambito del processo di gestione del ciclo passivo, valutazione della presenza di eventuali attività con impatti privacy;
2. avvio del processo di selezione del fornitore tenendo in debito conto i requisiti e le competenze minime definiti nel corso della fase 1, nonché gli obiettivi di sicurezza e privacy prefissati;
3. individuazione del ruolo privacy (titolare, contitolare o responsabile del trattamento di dati personali) da attribuire a fornitori/terze parti che vengono chiamati a trattare i dati personali;
4. formalizzazione del contratto e della corrispondente nomina a responsabile, secondo lo standard di riferimento.

Il processo si applica a tutte le tipologie di contratto/accordo, sia in prima istanza che in sede di rinnovo, nonché alle eventuali sub forniture.

Nell'ambito del processo di gestione dei responsabili del trattamento sono previste attività periodiche di monitoraggio, proporzionate all'oggetto del contratto e ai connessi rischi e impatti privacy.

In particolare, le funzioni di volta in volta competenti, con il supporto della Funzione Legal:

- revisionano ed esaminano gli accordi di nomina ex art. 28 GDPR, verificando il rispetto del GDPR in materia di responsabilità e obblighi dei Responsabili;
- con periodicità annuale, verificano lo stato di validità delle nomine effettuate procedendo, eventualmente, con le revoche del caso;
- con periodicità definita in base alle peculiarità del singolo incarico, effettuano verifiche a campione concernenti il rispetto da parte del Responsabile del trattamento delle istruzioni fornite e delle previsioni di legge, nonché del livello di implementazione delle misure di sicurezza.

3.1.5 Nomina di Solesi a responsabile

Nei casi in cui la Società svolga per conto di altri titolari attività di trattamento di dati personali, deve essere previsto, da parte del titolare, uno specifico atto che, al momento della stipula del contratto, nomini formalmente la Società quale responsabile del trattamento ai sensi dell'art. 28 del GDPR.

Tale accordo deve almeno:

- definire il perimetro di attività di trattamento affidate alla Società, individuando le relative responsabilità in relazione alle misure da garantire per la protezione e la tutela dei dati personali trattati e la conformità alle disposizioni normative;
- se del caso, prevedere una formula di autorizzazione generale o specifica, ai sensi dell'art. 28, par. 2 del GDPR, volta alla gestione delle nomine a Responsabile che la Società dovrà eventualmente formalizzare nei confronti dei propri fornitori coinvolti nelle attività di trattamento effettuate per conto di altri titolari (c.d. sub-responsabili);
- riportare l'indicazione relativa alla validità della stessa, in relazione alla durata del contratto.

4 Il trattamento di dati personali

Come anticipato in premessa, i principi di comportamento e le disposizioni generali disciplinate dalle presenti Linee Guida sono applicabili a tutti i trattamenti effettuati dalle singole Società, al fine di garantire la tutela dei diritti e delle libertà fondamentali di tutte le categorie di interessati.

In particolare, il GDPR definisce come

- **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;
- **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.

Nell'ambito delle proprie attività, il Titolare può trattare dati personali riferiti, a titolo esemplificativo e non esaustivo, alle seguenti categorie di interessati:

- candidati
- dipendenti
- fornitori
- clienti
- altri soggetti (es.: componenti organi societari, visitatori, collaboratori, ecc.).

Le tipologie di dati che la Società può trattare in relazione alle categorie di interessati sopra identificate sono evidenziate nel Registro dei trattamenti.

Trattamento di categorie particolari di dati personali

L'art 9 del GDPR individua alcune tipologie di dati, il cui trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali dell'interessato. All'interno di tali categorie particolari di dati personali sono inclusi:

- dati che rivelano
  - l'origine razziale o etnica;
  - le opinioni politiche;
  - le convinzioni religiose o filosofiche;
  - l'appartenenza sindacale;
- dati genetici;
- dati biometrici, che consentano l'identificazione in modo univoco di una persona fisica;
- dati relativi a
  - stato di salute;
  - vita sessuale;
  - orientamento sessuale.

Tali dati possono essere trattati solo ed esclusivamente se:

- l'interessato ha prestato il proprio consenso esplicito in relazione ad una o più finalità specifiche, salvo nei casi in cui la normativa applicabile, nazionale o sovranazionale, non lo consenta;

- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per:
  - adempiere ad obblighi e/o esercitare diritti specifici del Titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, laddove previsto dalla normativa applicabile, nazionale o sovranazionale, o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;
  - tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
  - accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni;
  - motivi di interesse pubblico rilevante sulla base del diritto nazionale o sovranazionale; l'interesse pubblico deve, comunque, risultare proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
  - finalità di medicina preventiva o medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero per la gestione dei sistemi e servizi sanitari o sociali sulla base del diritto nazionale o sovranazionale o conformemente al contratto con un professionista della sanità[3].

A tal fine, il Titolare:

- effettua trattamenti di categorie particolari di dati personali solo nelle casistiche tassativamente previste dall'art. 9 del GDPR, nel rispetto delle misure di garanzia previste dall'art. 2-*septies* del Codice Privacy;
- evidenzia il trattamento di tali dati, e le relative finalità e modalità, nei moduli di informativa sottoposti all'interessato;
- ove necessario, distingue nel modulo di consenso la richiesta del consenso al trattamento delle categorie particolari di dati personali;
- traccia all'interno del Registro *ex* art. 30 del GDPR, i trattamenti aventi ad oggetto i dati di cui trattasi;
- adotta adeguate misure di sicurezza.

Trattamento di dati relativi a condanne penali e reati

I dati personali attinenti condanne penali e reati possono essere trattati esclusivamente, previo consenso dell'interessato, nei casi previsti dalla normativa di riferimento, nazionale o sovranazionale, o sotto il controllo dell'autorità pubblica, laddove siano previste garanzie appropriate per i diritti e le libertà degli interessati.

In particolare, un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Laddove una società entri "accidentalmente" in possesso di dati personali relativi a condanne penali e reati (ad es., nell'ambito delle attività connesse alla gestione di un contenzioso), provvede tempestivamente a cancellare in via definitiva tali informazioni dai propri sistemi e dai documenti che le contengano, salvo disposizioni di legge applicabili che ne consentano il trattamento.

Per quel che concerne l'attività di raccolta e trasmissione alle stazioni appaltanti della documentazione necessaria ai fini della partecipazione a gare, a seguito delle recenti modifiche che hanno interessato la normativa di riferimento (codice dei contratti, normativa antimafia, ecc.), la Società provvede a trasmettere alle stazioni appaltanti i dati personali dei soggetti rilevanti, affinché siano le stesse stazioni appaltanti a procedere agli

[3] Ciò vale se e solo se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

accertamenti richiesti dalla legge.

I dati giudiziari eventualmente raccolti nell'ambito delle suddette attività in ottemperanza alla previgente normativa sono conservati nel rispetto di idonee misure di sicurezza, ivi inclusa la limitazione dei permessi di accesso a tali dati, ovvero cancellati, in assenza di prescrizioni di legge che ne impongano la conservazione.

5 Base legale del trattamento

Perché sia lecito, il trattamento di dati personali deve fondarsi su una delle basi legittime previste esplicitamente dal GDPR o da altre fonti legislative nazionali o sovranazionali, quali:

- ✓ consenso dell'interessato;
- ✓ esecuzione di un contratto di cui l'interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dello stesso (incluso il contratto di lavoro);
- ✓ adempimento di obblighi legali in capo al Titolare;
- ✓ salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
- ✓ esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- ✓ perseguimento del legittimo interesse del Titolare o di terzi, laddove non prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il Titolare procede all'analisi preventiva delle attività e operazioni che implicano il trattamento di dati personali, al fine di identificare la base legale più corretta su cui fondare il trattamento medesimo.

La base legale è censita nel Registro dei trattamenti, nonché debitamente evidenziata nelle informative sottoposte all'interessato.

Il consenso

Con il termine consenso si intende la manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con cui l'interessato stesso fornisce la propria autorizzazione al trattamento dei dati personali che lo riguardano.

Il consenso deve essere espresso mediante un atto positivo e inequivocabile con cui l'interessato manifesta l'intenzione libera, specifica, informata in merito al trattamento dei dati personali che lo riguardano.

Qualora il consenso dell'interessato sia prestato per iscritto, in una dichiarazione che riguarda anche altre questioni, la richiesta di consenso viene presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

la Società limita i casi di trattamento di dati personali basati sul consenso dell'interessato, in particolare nell'ambito del rapporto di lavoro, anche in considerazione delle indicazioni fornite in tal senso dalle Autorità garanti.

Nel dettaglio, la Società tratta dati personali in base al consenso dell'interessato nei seguenti casi:

- nell'ambito del processo di selezione e assunzione del personale, raccolta di *curriculum vitae* e svolgimento di colloqui e interviste con candidati, nei casi in cui siano eventualmente raccolti dati e informazioni ulteriori rispetto a quelli forniti spontaneamente dall'interessato nel CV;
- in tutti gli ulteriori trattamenti che implicano l'acquisizione di dati personali per i quali non sussistono altre basi giuridiche cui riferirsi (e.g., trattamento di acquisizione e trasmissione di foto/immagini dell'interessato, ad esempio, nel caso di partecipazione ad eventi, riprese televisive, ecc.) fermo restando che in nessun caso il mancato conferimento del consenso da parte del dipendente ha o può avere effetti negativi sul rapporto di lavoro in essere.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, fermo restando che tale revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

La Società al fine di dimostrare la *compliance* alle previsioni del Regolamento, nonché di garantire il corretto esercizio del diritto di revoca del consenso da parte dell'interessato:

- garantisce che l'interessato possa revocare il consenso con la stessa facilità con cui è stato accordato.
- assicura la debita tracciabilità e archiviazione dei consensi raccolti.

Legittimo interesse

Il legittimo interesse può costituire una base giuridica del trattamento di dati personali, ai sensi dell'art. 6 del GDPR, compreso l'eventuale legittimo interesse di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi, a condizione che questi non prevalgano sugli interessi o i diritti e le libertà fondamentali dell'interessato. Al riguardo, occorre tenere conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Ad esempio, potrebbero sussistere tali legittimi interessi nei casi in cui esiste una relazione pertinente e appropriata tra l'interessato e il Titolare (*i.e.*, l'interessato è un cliente del Titolare o è alle sue dipendenze). Può, altresì, costituire legittimo interesse del Titolare trattare dati personali strettamente necessari a fini di prevenzione delle frodi o a tutela del patrimonio aziendale (come ad es., nel caso di trattamento di dati personali relativi al traffico telefonico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione).

In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine.

Anche tenuto conto di quanto sopra evidenziato, Solesi, effettua, tra l'altro, trattamenti in base al proprio legittimo interesse con riferimento al trattamento di dati personali eventualmente raccolti nell'ambito delle attività di verifica aventi impatti sul sistema di controllo interno e il mantenimento della sua adeguatezza (attività sensibili ai fini del D.Lgs. n. 231/2001, controlli amministrativo-contabili). In particolare, in tali casi, l'interesse legittimo di Solesi risiede nello svolgimento di opportune verifiche volte ad accertare l'adeguatezza e l'efficacia del sistema di controllo interno, con riferimento sia alla Società che alle società da essa controllate.

Altri trattamenti condotti dalla Società sulla base del legittimo interesse possono essere, a titolo esemplificativo e non esaustivo:

- gestione dei sistemi informativi;
- acquisizione delle foto da apporre sul badge aziendale al fine di rilevare le presenze, per finalità di payroll e di sicurezza sul luogo di lavoro;
- utilizzo di cookie tecnici sul sito web aziendale.

6 Informativa

I principi di trattamento corretto e trasparente implicano che l'interessato sia debitamente informato in merito al trattamento di dati personali che lo riguardano.

Sul punto, il WP29 ha emesso delle specifiche Linee guida, su cui la Società si è basate ai fini della predisposizione dei moduli di informativa sottoposti all'interessato.

Informazioni da fornire qualora i dati siano raccolti presso l'interessato

Ai sensi dell'art. 13 del GDPR, la Società fornisce all'interessato, qualora i dati siano raccolti presso quest'ultimo, le seguenti informazioni:

- l'identità e i dati di contatto del Titolare;
- le finalità del trattamento cui sono destinati i dati personali;
- la base giuridica del trattamento, in particolare descrivendo l'eventuale legittimo interesse del Titolare;
- le modalità di trattamento, con particolare riferimento all'esistenza di un processo decisionale automatizzato, unitamente alle informazioni sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
- l'eventuale obbligo di fornire i dati personali, nonché le conseguenze del mancato conferimento dei dati stessi, in particolare laddove la comunicazione di dati personali rappresenti un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- gli eventuali destinatari/categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del Titolare di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale e l'esistenza di una decisione di adeguatezza della Commissione ovvero, nel caso dei trasferimenti di cui agli artt. 46, 47, o 49 del GDPR, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- l'esistenza del diritto dell'interessato di chiedere al Titolare l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'Autorità di controllo.

Tale condivisione deve avvenire al momento della raccolta dei dati.

Nei casi in cui l'interessato disponga già delle suddette informazioni, non è obbligatorio fornirgli tale informativa.

Informazioni da fornire qualora i dati non siano raccolti presso l'interessato

Qualora i dati non siano raccolti presso l'interessato, l'art. 14 del GDPR prevede che il Titolare fornisca all'interessato un'informativa che preveda, in aggiunta a quanto illustrato nel precedente paragrafo:

- le categorie di dati personali raccolte;
- l'indicazione delle fonti da cui si sono ottenuti tali dati.

Tali informazioni sono fornite all'interessato entro un termine ragionevole dall'ottenimento dei dati personali, e comunque entro un mese, tenendo conto delle specifiche circostanze in cui i dati sono raccolti.

Laddove i dati raccolti presso terzi siano destinati alla comunicazione con l'interessato, l'informativa dovrà essere resa al più tardi al momento della prima comunicazione.

Nel caso in cui i dati personali siano oggetto di comunicazione ad un altro destinatario, l'interessato dovrà essere informato non oltre la prima comunicazione.

Informazioni da fornire in caso di trattamenti per finalità ulteriore

Nel caso di trattamenti di dati personali per una finalità diversa da quella per cui essi sono stati raccolti, la Società, prima di tale ulteriore trattamento, fornisce all'interessato informazioni in merito a tale ulteriore finalità, unitamente alle altre informazioni necessarie.

Non è necessario imporre l'obbligo di fornire l'informazione qualora:

- l'interessato disponga già dell'informazione;
- la registrazione o la comunicazione dei dati personali siano previste per legge;
- nel caso in cui informare l'interessato si riveli impossibile o possa richiedere uno sforzo sproporzionato.

Aggiornamento delle informative

A seguito di eventuali modifiche apportate ai trattamenti di dati personali, debitamente censite nel relativo Registro dei trattamenti, il Titolare aggiorna tempestivamente i moduli di informativa.

In particolare, nel caso in cui si intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, prima di tale ulteriore trattamento la Società fornisce all'interessato il modulo di informativa aggiornato.

7 Gestione dei diritti degli interessati

Il GDPR, agli artt. 15-22 prevede specifici diritti riconosciuti all'interessato, di cui quest'ultimo deve essere debitamente informato da parte del Titolare.

In particolare, si prevede all'interno dei moduli di informativa un riferimento alla possibilità per l'interessato di rivolgersi alla Società che tratta i dati in questione al fine di richiedere l'esercizio dei diritti allo stesso riconosciuti dal GDPR, nonché i necessari dati di contatto. Eventuali richieste dell'interessato devono essere gestite in accordo ai requisiti previsti dalla normativa e descritti nel presente capitolo.

Il Titolare comunica, altresì, a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali richieste ricevute dall'interessato e le relative conseguenze sul trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Su richiesta dell'interessato, il Titolare è tenuto a comunicargli l'identità dei destinatari dei dati.

Al fine di ottemperare alle citate previsioni, la Società implementa apposite misure tecniche e organizzative che garantiscono la corretta ed efficiente gestione delle richieste pervenute dagli interessati. In particolare:

- dal momento di ricevimento della richiesta decorrono i termini per la risposta previsti dal Regolamento. Qualora nell'ambito della richiesta effettuata non sia possibile accertare l'identità dell'interessato, il Titolare, avvalendosi del supporto delle funzioni aziendali impattate, avvia il processo di integrazione della richiesta tramite recupero delle evidenze necessarie (quali, a seconda dei canali utilizzati, esibizione o invio di una copia di un documento d'identità in corso di validità). In questo caso, i tempi per la risposta decorrono dal momento del ricevimento della documentazione integrativa ai fini dell'accertamento di identità;
- il Titolare assicura il processo di gestione della richiesta ed il riscontro all'interessato entro un mese dal ricevimento della richiesta, con risposta scritta o con l'indicazione che, in virtù della sua complessità, verrà fornito riscontro entro i successivi due mesi;
- la Società, con il supporto delle funzioni aziendali competenti, dunque, valuta l'ammissibilità della richiesta pervenuta in termini di:
  - **interessati coinvolti** – l'interessato ha la possibilità di richiedere l'applicazione dei diritti sopracitati solo ai propri dati personali, delegando eventualmente altri interessati per la gestione della richiesta. In tal senso si verifica la completezza e la correttezza della documentazione a corredo della richiesta (es. copia del documento di identità e – in caso l'interessato si faccia assistere da un terzo – di una copia della relativa procura o delega);
  - **completezza** – qualora la documentazione non risulti essere completa, sarà chiesto per iscritto all'interessato l'invio di una copia di un documento di identità e – in caso l'interessato si faccia assistere da un terzo – di una copia della relativa procura o delega, entro un termine specifico di 15 giorni solari, precisando che in caso contrario non sarà possibile fornire alcun riscontro;
  - **applicabilità** – possibilità di applicazione della richiesta da parte della Società in linea con il principio di non lesione dei diritti e le libertà altrui o in relazione ai limiti tecnologici;
  - **ripetizione** – numerosità o frequenza con cui la richiesta è pervenuta da parte dell'interessato richiedente. Nei casi di più richieste può essere possibile richiedere un contributo spese all'interessato per l'evasione della richiesta stessa. In tal senso si verifica se la richiesta è suscettibile di attribuzione di un contributo spese per gli eventuali costi amministrativi da sostenere, valutando se le richieste sono manifestamente eccessive, in particolare per il loro carattere ripetitivo;
  - **competenza** – i dati o i trattamenti su cui è richiesta l'applicazione dei diritti sono gestiti dalla singola Società in qualità di Titolare oppure di Responsabile del trattamento;
- per la valutazione degli aspetti di natura tecnologica, è coinvolta la Funzione IT.

Valutata l'ammissibilità, la Società alternativamente:

- procede con le attività di evasione della richiesta;

- procede con la comunicazione all'interessato dell'inammissibilità della richiesta e delle motivazioni alla base della valutazione effettuata;
- procede, nel caso dovesse emergere che i dati oggetto della richiesta sono trattati in qualità di Responsabile del trattamento, immediatamente ad inoltrare la richiesta al titolare del trattamento corrispondente.

Diritto di accesso ai dati

L'art. 15 del GDPR introduce il diritto degli interessati di accesso ai dati, ossia il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi od organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al Titolare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano ovvero di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'Autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nel caso in cui i dati personali siano trasferiti a un Paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza delle garanzie adeguate ai sensi del GDPR.

L'interessato ha il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ove possibile, il Titolare può fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali.

Il Titolare adotta tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online. Ciò vale in particolare qualora il Titolare tratti una notevole quantità d'informazioni riguardanti l'interessato; in tal caso, l'interessato deve precisare, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.

Il Titolare deve fornire una copia dei dati personali oggetto di trattamento, ove richiesto. In caso di ulteriori copie richieste dall'interessato, il Titolare può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni devono essere fornite in un formato elettronico di uso comune.

Diritto di rettifica dei dati

L'art. 16 del GDPR introduce il diritto degli interessati di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha altresì il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto all'oblio

L'art. 17 del GDPR introduce il diritto degli interessati all'oblio, ossia il diritto di richiedere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, qualora sussista uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento per motivi connessi alla sua situazione particolare e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al per finalità di marketing diretto;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto, nazionale o sovranazionale, cui è soggetto il Titolare;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione[4] ai minori, previo consenso del minore che abbia compiuto almeno 14 anni, ovvero di chi esercita la potestà genitoriale.

Nel caso in cui siano stati resi pubblici dati personali, il Titolare è obbligato a cancellarli e, tenendo conto della tecnologia disponibile e dei costi di attuazione, ad adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali oggetto della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Tale diritto non si applica nella misura in cui il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto nazionale o sovranazionale cui è soggetto il Titolare o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;
- per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'art. 89 del GDPR, nella misura in cui tale diritto rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di limitazione del trattamento

L'art. 18 del GDPR introduce il diritto degli interessati di limitazione al trattamento dei dati, quando ricorre una delle seguenti ipotesi:

[4] I "servizi della società dell'informazione" sono definiti dall'art. 1, par. 1, lett. b) della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, cui il GDPR espressamente rinvia.
Trattasi, in particolare, di "*qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi*", vale a dire, un servizio fornito senza la presenza simultanea delle parti ("*a distanza*"), mediante trasmissione di dati su richiesta individuale ("*a richiesta individuale di un destinatario di servizi*"), inviati all'origine e ricevuti a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che sono interamente trasmessi, inoltrati e ricevuti mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici ("*per via elettronica*").

- l'interessato contesta l'esattezza dei dati personali che lo riguardano, per il periodo necessario al Titolare per verificare l'esattezza di tali dati;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il Titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento ai sensi dell'art. 21 del GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare rispetto a quelli dell'interessato.

Di seguito si illustrano alcune modalità per limitare il trattamento dei dati personali:

- trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- rendere i dati personali selezionati inaccessibili agli utenti o rimuovere temporaneamente i dati pubblicati da un sito web;
- nel caso di archivi automatizzati, adottare dispositivi tecnici al fine di assicurare che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati.

Qualora venga attuata una limitazione al trattamento dei dati, tali dati personali devono essere trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

Diritto alla portabilità dei dati

L'art. 20 del GDPR introduce il diritto degli interessati alla portabilità dei dati personali che li riguardano, ossia il diritto degli interessati di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare senza impedimenti da parte del titolare cui li ha forniti, qualora:

- il trattamento si basi sul consenso o sia necessario ai fini dell'esecuzione di un contratto; e
- il trattamento sia effettuato con mezzi automatizzati.

Il Titolare, nel rispetto del diritto di portabilità dei dati, si impegna ad evitare il recupero e la trasmissione a un nuovo titolare di informazioni contenenti i dati personali di altri interessati che a ciò non hanno acconsentito, qualora sia verosimile che tali dati siano trattati secondo modalità in grado di ledere i diritti e le libertà dei terzi interessati in questione.

Il Titolare può trasmettere i dati personali forniti dagli interessati in un formato tale da non rivelare informazioni commerciali riservate o soggette a diritti di proprietà intellettuale.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato può ottenere la trasmissione diretta dei dati personali dal Titolare ad un altro titolare del trattamento, se tecnicamente fattibile. Tale trasmissione diretta dei dati può avvenire solo se è possibile instaurare una comunicazione fra due sistemi informativi, in modo sicuro, e se il sistema ricevente è tecnicamente in grado di ricevere i dati in ingresso. Qualora impedimenti di ordine tecnico precludano la trasmissione diretta, il Titolare deve illustrarne l'esistenza agli interessati.

Diritto di opposizione al trattamento

L'art. 21 del GDPR introduce il diritto dell'interessato di opposizione al trattamento dei dati personali, in qualsiasi momento, per motivi connessi alla sua situazione particolare, compresa la "profilazione". Ciò vale nel caso di trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, o per il perseguimento del legittimo interesse del Titolare medesimo o di terzi.

Il Titolare si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato

oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione, nella misura in cui sia connessa a tale attività di marketing diretto. In tal caso, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di opposizione al trattamento deve essere esplicitamente portato all'attenzione dell'interessato chiaramente e separatamente da qualsiasi altra informazione, al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Processo decisionale automatizzato

L'art. 22 del GDPR introduce il diritto degli interessati di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che li riguardano o che incida in modo analogo significativamente sulla loro persona. Tale diritto non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il Titolare;
- si basi sul consenso esplicito dell'interessato;
- sia autorizzata dal diritto nazionale o sovranazionale cui è soggetto il Titolare, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Tale trattamento comprende la "profilazione", laddove ciò produca effetti giuridici che riguardano l'interessato o incida in modo analogo significativamente sulla sua persona, che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica al fine di analizzare o prevedere aspetti riguardanti, ad esempio, il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.

Per quanto relativo alle prime due casistiche, il Titolare attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del Titolare, di esprimere la propria opinione e di contestare la decisione.

Tali decisioni non si devono basare sulle categorie particolari di dati personali (cfr., al riguardo, il par. 4.1 delle presenti Linee Guida), a meno che non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

8 Registro dei trattamenti

Il Titolare e il Responsabile del trattamento, nonché, ove applicabile, il Rappresentante del titolare nell'UE, predispongono e mantengono un Registro dei trattamenti, ossia un documento (anche in formato elettronico) in cui sono censite le attività di trattamento dallo stesso effettuate.

In esito all'analisi delle attività di trattamento esistenti e del ruolo di volta in volta ricoperto rispetto agli stessi, la Società ha adottato il Registro in qualità di Titolare del trattamento.

In dettaglio, il Registro dei trattamenti contiene le seguenti informazioni:

- il nome e i dati di contatto del Titolare;
- la descrizione sintetica delle attività svolte nell'ambito di ciascun trattamento;
- le funzioni aziendali di riferimento e gli eventuali Responsabili del trattamento;
- la base legale e la finalità del trattamento;
- le categorie di interessati e l'indicazione delle categorie di dati personali;
- le modalità di trattamento dei dati personali e gli strumenti utilizzati;
- le categorie di destinatari a cui i dati personali sono comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- 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 l'indicazione dell'esistenza delle relative decisioni di adeguatezza della Commissione;
- ove possibile, i termini ultimi previsti per la cancellazione dei dati personali.

/Il Registro dei trattamenti svolge un ruolo di primaria importanza nel governo delle attività di trattamento, in quanto consente di:

- identificare tutte le attività di trattamento svolte dalla Società;
- esercitare un governo puntuale sui dati personali gestiti;
- individuare i trattamenti con un rischio elevato per i diritti e le libertà delle persone fisiche oggetto del trattamento;
- rispondere efficacemente alle richieste di applicazione dei diritti dell'interessato;
- verificare la conformità ai requisiti normativi.

La Società ha, altresì, definito i ruoli e le responsabilità connessi alla gestione del Registro, nonché della sua struttura e delle informazioni in esso inserite.

Ruoli e responsabilità

Tutte le Funzioni aziendali collaborano e supportano il Titolare nell'aggiornamento del registro dei trattamenti, sulla base delle informazioni fornite dai vari uffici o unità che trattano dati personali; ciascun Responsabile di funzione, in relazione ai trattamenti di propria competenza, riveste un ruolo operativo nelle suddette attività di gestione e mantenimento del Registro dei trattamenti.

In particolare, ciascun Responsabile di Funzione verifica periodicamente la correttezza e l'efficacia delle attività di gestione del Registro e del livello di aggiornamento delle informazioni relative ai trattamenti censiti.

Ciascun Responsabile di funzione, dunque, per quanto di propria competenza:

— monitora la necessità di censire nuovi trattamenti nel Registro;

— monitora, con cadenza almeno semestrale e comunque ogni qual volta necessario, lo stato di aggiornamento del Registro, anche coordinandosi con i propri collaboratori/incaricati, al fine di garantire l'allineamento delle informazioni in esso contenute ad eventuali cambiamenti intervenuti nell'ambito delle operazioni di

trattamento di dati personali effettuate (a titolo esemplificativo, modifiche inerenti la finalità, i tempi di conservazione, i fornitori esterni e le funzioni interne coinvolte, i sistemi utilizzati, ecc.);

— richiede supporto alla Funzione IT nell'identificazione delle misure di sicurezza associate ai trattamenti censiti nel Registro.

In esito al processo di aggiornamento delle informazioni contenute nel Registro dei trattamenti, l'organo amministrativo, ovvero il soggetto all'uopo incaricato, valida il Registro medesimo.

La struttura del registro dei trattamenti

Il Registro dei trattamenti consiste in una tabella in formato *excel* completa di tutte le informazioni richieste dall'art. 30 del GDPR, nonché delle ulteriori informazioni ritenute utili per il governo ed il monitoraggio delle attività di trattamento di dati personali.

Per ciascun trattamento svolto dalla Società, in qualità di Titolare, il Registro riporta le informazioni indicate al par. 8, che possono essere classificate nei seguenti macro-ambiti:

- riferimenti di carattere generale, quali la descrizione del trattamento, le funzioni interne che eseguono le operazioni principali sui dati oggetto di trattamento, l'elenco dei processi della Società su cui il trattamento ha impatto;
- elementi di maggior livello di dettaglio relativi alle operazioni di trattamento, quali le finalità, la base legale, la tipologia di dati, i termini ultimi per la cancellazione, le categorie di interessati, nonché i sistemi applicativi e/o archivi cartacei utilizzati, l'indicazione degli eventuali responsabili del trattamento;
- ulteriori dettagli in merito all'eventuale trasferimento extra-UE dei dati personali, inclusa l'indicazione dei soggetti destinatari, del Paese di destinazione e dei presupposti di liceità del trasferimento medesimo.
- eventuali dati relativi a terze parti coinvolte nel trattamento a cui vengono comunicati i dati.

9 Violazioni dei dati personali (*Data Breach*)

Gli incidenti a livello privacy si configurano come una 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.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni materiali o immateriali alle persone fisiche (a titolo esemplificativo, perdita del controllo dei dati personali che le riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata, ecc.).

Ai fini del GDPR, si considerano incidenti di privacy gli eventi che mettano a rischio, anche in maniera accidentale, i dati personali trattati in qualsiasi formato, quali, a titolo esemplificativo e non esaustivo:

- l'aggiramento dei controlli di sicurezza di un sistema informatico per avere accesso ai dati personali senza autorizzazione;
- la perdita di un dispositivo di memorizzazione elettronica (ad es. CD, DVD, *laptop*, *hard disk*, *tablet*) contenente dati personali non crittografati;
- le e-mail di *phishing* aperte o utilizzate da un dipendente che hanno generato una perdita o un accesso non autorizzato ai dati personali o che hanno permesso l'installazione di un *malware* che sottrae dati;
- le e-mail contenenti dati personali inviata involontariamente al mittente sbagliato;
- i difetti di protezione dei *software* che possono aver provocato un accesso non autorizzato ai sistemi o ai dati personali;
- la modifica o cancellazione impropria di dati personali.

In caso di violazione dei dati personali, la Società che ha subìto la violazione deve notificare la stessa all'Autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, salvi i casi in cui dimostri, in accordo al principio di responsabilizzazione, che la violazione non comporta rischi per i diritti e le libertà degli interessati.

Qualora tale notifica avvenga oltre il termine delle 72 ore, la Società dovrà fornire le ragioni di tale ritardo.

Qualora la violazione dei dati sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, è necessario informare tempestivamente anche gli interessati stessi, al fine di consentirgli di prendere le precauzioni necessarie, in stretta collaborazione con l'Autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità.

La notifica verso gli interessati non è richiesta qualora la Società abbia:

- messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

La comunicazione agli interessati non è dovuta anche qualora provvedervi richiederebbe uno sforzo sproporzionato. In tal caso, si può procedere a una comunicazione pubblica o a provvedimenti simili, affinché gli interessati siano informati con analoga efficacia.

Il Titolare deve inoltre documentare qualsiasi violazione di dati personali subita, anche laddove non ricorrano i presupposti per la notifica all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze, conseguenze e i provvedimenti adottati.

Sulla base di quanto sopra, la Società ha adottato un'apposita procedura organizzativa, "*Gestione degli eventi di violazione ai dati personali (Data Breach)*" cui si rinvia, la quale prevede, tra l'altro, la tenuta di un apposito inventario delle eventuali violazioni riscontrate, al fine di garantire idonea tracciabilità alle stesse.

10 Analisi dei rischi e Data Protection Impact Analysis (DPIA)

La Società stabilisce lo svolgimento di una valutazione preliminare degli impatti di un trattamento sulla protezione dei dati personali nei casi in cui lo stesso presenti un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura, dell'oggetto, del contesto, delle finalità del trattamento e dell'uso eventuale di nuove tecnologie.

Nel rispetto di quanto previsto dall'art. 35 del GDPR, il modello di valutazione contiene almeno i seguenti elementi:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone coinvolte.

Al fine di ottemperare ai requisiti sopra descritti, è stato definito un approccio metodologico di analisi del rischio privacy che si struttura in due fasi distinte:

- valutazione preliminare del rischio intrinseco associato al trattamento;
- valutazione del livello di implementazione delle misure di sicurezza a presidio dei rischi identificati nella fase precedente e determinazione del rischio residuo.

Secondo tale metodologia di valutazione del rischio, le Funzioni aziendali attivano il processo di *privacy by design* (cfr. par. 2.1) e, se del caso, la DPIA, nel rispetto di quanto descritto nella specifica procedura, nei casi in cui si preveda a titolo esemplificativo e non esaustivo:

- lo sviluppo di un nuovo progetto che comporta un trattamento di dati personali;
- un intervento significativo sugli applicativi esistenti che trattano o potrebbero trattare dati personali;
- una modifica ad un processo di business esistente che potrebbe modificare le attività di trattamento dei dati personali o richiederne nuove;
- l'attività di esternalizzazione di servizi che prevedono il trattamento di dati personali;
- una qualsiasi attività che potrebbe avere un impatto diretto sui trattamenti di dati personali esistenti.

Qualora il trattamento sia svolto in tutto o in parte da un Responsabile del trattamento, quest'ultimo deve assistere il Titolare nel processo fornendo ogni informazione necessaria.

Sulla base delle informazioni raccolte, le funzioni aziendali, con il supporto della funzione IT, valutano:

- la limitazione delle finalità (specifiche, esplicite e legittime) del trattamento;
- il principio di minimizzazione dei dati (es. periodo di conservazione dei dati, pseudonimizzazione, minimizzazione dell'accesso ai dati).

Tale valutazione (c.d. *Privacy Impact Assessment*, di seguito anche PIA), consente di considerare, prima che il trattamento venga posto in essere, il rischio, ossia l'incidenza, delle attività poste in essere dal Titolare sui dati personali.

Tuttavia, il *Privacy Impact Assessment* non si esaurisce nel processo di *Privacy by Design*, ma è da intendersi come un processo continuativo che deve essere condotto iterativamente sul trattamento ogni qualvolta questo subisca una variazione significativa.

Se, a seguito delle analisi svolte, il livello di rischio determinato rimane alto e senza misure specifiche per mitigare detto rischio, il Titolare può richiedere la consultazione preventiva all'Autorità di controllo trasmettendogli formale comunicazione, ossia presentando la relazione sul Privacy Impact Assessment svolto.

L'Autorità è tenuta a fornire, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto, a fronte del quale il Titolare/Delegato del Titolare valuta eventuali altre azioni da mettere in atto per procedere al trattamento o, in alternativa, se non è grado di adempiere alle indicazioni fornite dall'Autorità, decide di non avviare il trattamento o di bloccare un trattamento esistente.

Tutte le funzioni operative e di business, con il supporto della Funzione IT ove necessario, effettuano una revisione periodica di tutti trattamenti ad alto rischio sottoponendoli al processo di DPIA almeno ogni tre anni e comunque in funzione dell'evolversi dei rischi per i diritti e le libertà degli interessati.

11 Misure di sicurezza

In ottemperanza all'art. 32 del GDPR, il Titolare ha l'onere di implementare misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio. In particolare, l'articolo citato prevede che siano attuate, se del caso, le seguenti misure di sicurezza:

- pseudonimizzazione[5] e cifratura dei dati personali;
- capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Con il supporto della funzione IT, il Titolare ha stabilito i seguenti principi e misure di controllo.

Gestione delle credenziali di autenticazione

- hanno diritto all'utilizzo degli strumenti informatici e ai relativi accessi solo le risorse che per funzioni lavorative ne abbiano un effettivo e concreto bisogno;
- sono previsti dei profili di autorizzazione che consentono, ove opportuno, l'accesso differenziato, per incaricato o per classi omogenee di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento di competenza; la configurazione, aggiornamento e gestione dei profili di autorizzazione è di competenza della Funzione IT, su impulso del Responsabile di Funzione cui riferisce l'incaricato.
- Le credenziali di autenticazione per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se autorizzati al trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al proprio responsabile gerarchico, il quale concederà tale autorizzazione in base alle specifiche indicazioni ricevute dal titolare o dal responsabile del trattamento
- il lavoratore ha l'obbligo di utilizzare solo ed esclusivamente le aree di memoria dei server e quelle di gruppo di lavoro (i.e. cartelle di rete), ed ivi creare e conservare file o archivi di dati;
- il Personal Computer (PC) in uso al lavoratore contiene tutti i software necessari a svolgere le mansioni affidate. L'accesso al pc è regolato mediante l'inserimento di specifica password personale e da considerarsi strettamente riservata;
- Non è consentito:
  - modificare le configurazioni già impostate sul pc consegnato;
  - utilizzare/scaricare programmi senza la preventiva autorizzazione del superiore gerarchico e del Responsabile IT;
  - installare alcun software di cui la Società non possieda la licenza;
  - aggiungere o collegare dispositivi hardware (hard disk, driver, etc.), periferiche (telecamere, chiavi usb, ecc.) diversi da quelli consegnati, senza l'autorizzazione dell'IT.

Come scegliere e usare la password:

- [usare almeno otto caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.

[5] Si precisa che l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della pseudonimizzazione nel GDPR non è tuttavia intesa a precludere altre misure di protezione dei dati.

- usare lettere, di cui almeno una maiuscola, numeri e almeno un carattere speciale tra . ; $! @ - > <, etc.]
- non utilizzare date di nascita, nomi o cognomi propri o di parenti o altre parole facilmente ricostruibili
- non sceglierla uguale alla matricola o alla user-id
- custodirla sempre in un luogo sicuro e non accessibile a terzi
- non divulgarla a terzi
- non condividerla con altri utenti

Gestione delle strumentazioni e dotazioni informatiche aziendali

Le strumentazioni informatiche aziendali fornite e tutte le dotazioni che contengono informazioni confidenziali devono essere custodite con la massima diligenza ed utilizzate in modo tale da preservarne le funzionalità, riducendo al contempo i rischi di danneggiamento e/o malfunzionamento.

Questi strumenti sono forniti a scopo lavorativo. Per motivi di sicurezza, di *compliance* normativa e senza ricadere in alcun modo nelle casistiche di controllo a distanza di cui all'art. 4 della Legge 300/70, il Titolare si riserva il diritto di monitorare l'utilizzo di tali risorse. Il Titolare potrà esercitare tale diritto in qualsiasi momento e senza preavviso, con lo scopo di valutare la conformità alle *policy*, alla sicurezza ed integrità delle proprie informazioni, nonché alle leggi ed ai regolamenti applicabili. Come, peraltro, indicato nelle lettere di informativa.

Le risorse IT assegnate devono essere utilizzate per le finalità lavorative. L'eventuale utilizzo personale delle stesse da parte del lavoratore è tollerato nella misura in cui tale utilizzo è occasionale e non viola le procedure aziendali e/o le normative applicabili. In nessun caso, peraltro, è consentito:

- utilizzare eccessivamente le risorse aziendali in termini di occupazione di spazio sui server, sui personal computer, del canale Internet e della posta elettronica.
- interferire con la produttività individuale propria e altrui.
- impedire le attività di business della Società.
- generare qualsiasi azione che possa compromettere la reputazione della Società.

Non è consentito, salvo preventiva espressa autorizzazione della Funzione IT, modificare le caratteristiche impostate sul proprio PC, né procedere ad installare dispositivi di carattere personale di memorizzazione, comunicazione o altro (i.e. masterizzatori, modem, telefoni cellulari, hard disk, USB drive, schede di memoria, etc.).

Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password. Il PC deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate o in caso di suo inutilizzo. In ogni caso, anche per brevi assenze o inutilizzi, è obbligatorio l'utilizzo di uno "screensaver" a tempo che si attivi dopo non più di 2 minuti di inattività e con l'obbligo di reintrodurre la password di accesso.

Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

Il Personale non può collegare apparati di rete non autorizzati alla rete aziendale e non deve attivare alcun servizio non autorizzato, specialmente *Hotspot wireless*. Solo i dispositivi approvati ed installati dalla Funzione IT, possono essere connessi alle reti della Società o utilizzati per gestire le informazioni di proprietà dello stesso.

L'accesso, o anche solo il tentativo di accesso, ai sistemi interni, alle reti e/o ai servizi erogati dalla Società utilizzando dispositivi non forniti dallo stesso (es.: computer, tablet o smartphone), è vietato.

L'accesso da remoto alle risorse informatiche può avvenire solo tramite l'utilizzo di metodi sicuri ed approvati dalla Funzione IT (ad esempio VPN, servizi resi disponibili verso l'esterno come la *Web Mail*, ecc.).

Cancellazione dei dati dai pc e/o da altri supporti rimovibili

I dati personali conservati sui PC e/o altri supporti rimovibili (i.e. dischetti, CD, DVD, supporti USB, hard disk, etc.) devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare tali PC e supporti ad usi

diversi e/o in conformità alla normativa RAEE nel caso siano destinati a smaltimento.

Per tutto quanto concerne l'architettura informatica e le ulteriori disposizioni e misure di sicurezza previste (i.e. back-up, ecc.) si rinvia alle specifiche istruzioni e/o policy aziendali in tema di sistemi e strumenti informatici, il cui aggiornamento è a cura della funzione IT.

Strumenti removibili e Mobile Device

Al Personale autorizzato sono assegnate risorse informatiche (*removable media*) per il trasferimento ed il salvataggio temporaneo delle informazioni, quali: supporti USB, schede di memoria SD e micro SD. I dati e le informazioni devono essere conservati su tali dispositivi solo in via temporanea e, alla fine del loro utilizzo, devono essere cancellati in modo che non possano essere più recuperati. I supporti rimovibili per il salvataggio dei dati devono essere criptati mediante l'utilizzo di un apposito software installato su tutte le postazioni di lavoro.

Per *Mobile Device* (dispositivi mobili) si intendono dispositivi quali smartphone, palmari, tablet, ecc. che siano di proprietà della Società o personali (ove autorizzati).

È compito di ciascun utente mantenere aggiornato il sistema operativo del *Mobile Device* in base ai rilasci messi a disposizione dal fornitore ma non senza aver verificato preventivamente con l'IT la presenza di eventuali controindicazioni.

La SIM societaria viene fornita al Personale congiuntamente ad uno *smartphone* aziendale. Per ragioni di sicurezza, non è consentito l'utilizzo della SIM societaria su uno *smartphone* personale.

Lo smaltimento di *smartphone* e di tutti gli *asset* forniti e contenenti informazioni della Società, deve essere effettuato in modo tale da rendere impossibile il recupero delle informazioni stesse ed in linea con il processo delineato nella procedura di smaltimento dei dispositivi. Questo può avvenire tramite la distruzione fisica del supporto o mediante una formattazione a basso livello dello stesso, come menzionato anche nella normativa sulla Privacy (Regolamento UE 679/2016).

Al fine di evitare infezioni da *malware*, il Personale deve fare molta attenzione quando scarica contenuti da Internet o quando riceve dati o link da altre persone tramite e-mail e qualunque altro canale di comunicazione o servizio, compresi gli SMS.

Al termine della collaborazione con la Società, il Personale dovrà restituire alla Società tutti i beni assegnati in ragione del rapporto di lavoro.

Software

I software installati sugli apparati elettronici di tutto il Personale devono soddisfare e rispettare i requisiti di legge, le regole, gli standard professionali e tutte le procedure e i manuali aziendali. A tal proposito, la Società si riserva il diritto di intraprendere ogni attività ritenuta opportuna al fine di garantire il rispetto delle fonti citate, ad esempio mediante il monitoraggio e/o la rimozione di qualunque software, file o informazione presente sui dispositivi da essa gestiti (es. computer, dispositivi di memorizzazione, server) che non rispetti le leggi e/o le policy aziendali.

Gli apparati elettronici consegnati dalla Società sono equipaggiati con una suite standard di programmi commerciali provvisti di regolare licenza e/o di proprietà della Società. Tutto il Personale è responsabile del rispetto di tutte le leggi vigenti, i regolamenti e termini di licenza che accompagnano il software, inclusa la restrizione di copia o modifica del software e della documentazione associata.

I software approvati e la documentazione ad essi associata possono essere riprodotti solo con l'approvazione della Funzione IT. Qualunque software duplicato in violazione alle licenze d'uso o in violazione delle policy aziendali non può essere installato o utilizzato.

Ciascun lavoratore:

- deve accertarsi che i sistemi antivirus e antispyware presenti sul proprio computer, le patch di sicurezza ed i software risultino sempre aggiornati. In condizioni di normale funzionamento, gli aggiornamenti dei software standard aziendali sono automatici e avvengono nel momento in cui l'utente è connesso alla rete aziendale, in VPN e, in ogni caso, ogni volta in cui è connesso ad internet. In caso di malfunzionamenti relativi l'aggiornamento dei software sul proprio computer, avvisare prontamente la Funzione IT.

— deve informare immediatamente la Funzione IT qualora si sospetti, a seguito di comportamenti anomali dei dispositivi informatici, della possibile infezione dovuta al veicolarsi di codice malevolo ed evitare di tentare di risolvere il problema in autonomia. A tal proposito, è necessario porre particolare attenzione ad aventi che potrebbero indicare la presenza di un'infezione del dispositivo (ad es. perdita o modifica di dati o file, rallentamento delle prestazioni, cambiamenti di nome dei dischi, presenza di programmi non installati dall'utente, apertura casuale di pagine web, criptazione di file con richiesta di riscatto, ecc.).

Comunicazioni elettroniche, navigazione Internet

La Società mette a disposizione del suo Personale, risorse IT per comunicare elettronicamente in modo affidabile, in linea con i requisiti normativi e di business. Solo i metodi di comunicazione approvati dalla Società (come, ad esempio, la posta elettronica aziendale) possono essere usati per comunicazioni di lavoro.

Nella gestione della posta elettronica è fatto obbligo di:

- non aprire messaggi con allegati di cui non si conosce l'origine, che potrebbero contenere virus in grado di cancellare i dati sul PC.
- evitare di aprire filmati e presentazioni non attinenti all'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul PC.

Quando si effettua *un meeting on-line* condividendo il video o delle applicazioni, il Personale deve assicurarsi che solo le persone invitate siano collegate e che vedano solo le informazioni relative al *meeting*.

Nell'utilizzo di internet:

- è fatto divieto di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete della Società. I software necessari all'attività lavorativa vanno richiesti alle competenti strutture interne.
- usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti. Al proposito, a titolo puramente esemplificativo, non è consentito utilizzare internet per:
    - l'upload o il download di software gratuiti e *shareware* non autorizzati;
    - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
    - la partecipazione a Forum non professionali, l'utilizzo di chat on-line (esclusi gli strumenti autorizzati), di bacheche elettroniche anche utilizzando pseudonimi (o nicknames);
    - leggere le caselle personali esterne via *webmail* in quanto alcuni provider esterni non proteggono dai virus.
- al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società ha adottato uno specifico sistema di blocco o filtro automatico (firewall) che previene determinate operazioni di upload, download o l'accesso a determinati siti considerati non sicuri e/o comunque non attinenti alle attività aziendali.
- la Società, al fine di garantire la sicurezza e salvaguardia del sistema informatico aziendale, può effettuare controlli anche sulle corrette modalità di navigazione mediante l'utilizzo di sistemi di *proxy server o file di log*. Tali controlli non sono continuativi ed i file di log sono conservati per tempi limitati necessari al perseguimento esclusivamente delle finalità di sicurezza informatica dell'azienda.

Segnalazione Incidenti di Sicurezza

In accordo con le procedure aziendali, ogni incidente di sicurezza deve essere immediatamente identificato e riportato alla Funzione IT, in modo che possano essere applicate il più velocemente possibile le appropriate azioni correttive.

Il furto/smarrimento di qualunque dispositivo IT utilizzato per lavoro è considerato un incidente di sicurezza. A fronte di tale avvenimento il personale deve immediatamente segnalarlo alla Funzione IT. Inoltre, l'utente deve effettuare la denuncia del furto o smarrimento all'Autorità di pubblica sicurezza fornendone copia alla Funzione IT. Questi adempimenti sono propedeutici alla sostituzione delle risorse informatiche non più disponibili.

Il furto o lo smarrimento di informazioni della Società o informazioni relative a terze parti e/o clienti che includono ad esempio dati su computer, *tablet, smartphone*, supporti USB, DVD o altri supporti di memoria è considerato un incidente informatico e deve essere prontamente segnalato seguendo quanto previsto dalle vigenti normative aziendali in materia. L'utente deve segnalare quanto prima l'incidente di sicurezza alla Funzione IT, oltre che al proprio superiore gerarchico. Lo stesso vale per le informazioni cartacee.

Attività inusuali dei dispositivi IT, riconducibili a virus che comportino la perdita dei dati, la compromissione della riservatezza e l'interruzione del servizio (che sono considerati un incidente informatico), devono essere immediatamente riportate alla Funzione IT. Si ricorda che i file infetti contenuti negli allegati delle e-mail in arrivo e bloccati dal sistema antivirus non sono considerati un incidente.

La ricezione di qualsiasi comunicazione e-mail o SMS riconducile anche potenzialmente ad attività di *Phishing* sono da segnalare prontamente alla Funzione IT.

Lo smarrimento o il furto del badge possono causare rischi di accessi non autorizzati ai locali della Società. Una volta accertato lo smarrimento o il furto del badge, è necessario contattare immediatamente l'Ufficio Amministrazione del Personale in modo da bloccarne la funzionalità.

Qualora l'incidente di sicurezza segnalato possa determinare rischi di sicurezza sui dati personali degli interessati coinvolti, il segnalante con il supporto della Funzione IT dovrà attivare la procedura di *Data Breach* (cfr. par. 9 delle presenti Linee Guida).

12 Trasferimenti di dati al di fuori dell'UE

Il GDPR disciplina le modalità e i casi in cui può aver luogo il trasferimento di dati personali verso un Paese extra-UE o un'organizzazione internazionale, con particolare riferimento alle garanzie adeguate che consentono di procedere a detto trasferimento senza necessità di acquisire autorizzazioni specifiche da parte di un'Autorità di controllo e alle eventuali deroghe.

In riferimento a quanto sopra, si precisa che, ad oggi, Solesi non effettua trasferimenti di dati personali al di fuori dell'UE.

Più in particolare il trasferimento dei dati all'estero può rendersi necessario per ottenere visti di ingresso e permessi di soggiorno nei Paesi in cui il lavoratore può essere inviato in trasferta, nonché per tutte le operazioni legate a viaggi all'estero. Il trasferimento avrà ad oggetto i dati contenuti nel passaporto o gli altri dati, anche inclusi nelle cc.dd. categorie particolari, eventualmente richiesti dall'autorità del Paese di destinazione.

In relazione a ciascun caso specifico, il dipendente sarà informato in merito all'intenzione del Titolare di trasferire i suoi dati personali a un Paese terzo o a un'organizzazione internazionale e all'eventuale esistenza di una decisione di adeguatezza della Commissione o delle altre garanzie adeguate previste dagli artt. 46 e ss. del GDPR, nonché in merito ai mezzi posti a disposizione dell'interessato per ottenere una copia di tali dati o il luogo in cui gli stessi sono stati resi disponibili.

Laddove ricorrano i casi previsti dall'art. 49, par. 1, lett. a) del GDPR (inerente i casi in cui il trasferimento di dati personali verso Paesi extra-UE sia basato sul consenso dell'interessato, in assenza delle altre garanzie sopra indicate), il conferimento del consenso da parte dell'interessato può avere conseguenze sulla possibilità per il Titolare di trasmettere al Paese destinatario i dati necessari per l'esecuzione delle attività previste nel singolo caso di specie.

Le informazioni relative all'eventuale trasferimento dei dati al di fuori dell'UE vengono riportate all'interno del Registro dei trattamenti, in relazione a ciascuna attività di trattamento ivi censita.

13 Gestione delle relazioni con le Autorità di controllo

Il Titolare è tenuto a collaborare con le Autorità di controllo competenti nell'esecuzione dei suoi compiti, qualora richiesto.

In particolare, ai sensi degli artt. 30-33 e 36 del GDPR, il Titolare deve:

- mettere a disposizione dell'Autorità di controllo il Registro dei trattamenti, qualora richiesto;
- notificare qualsiasi violazione dei dati personali all'Autorità di controllo nelle casistiche e conformemente alle procedure già descritte nel cap. 9 delle presenti Linee Guida;
- procedere alla consultazione con l'Autorità di controllo qualora dallo svolgimento della DPIA emerga un rischio elevato con riferimento ad un trattamento di dati personali.

Il Titolare, tramite una corretta gestione della documentazione rilevante, rende disponibili al Garante tutte le informazioni e i documenti richiesti nell'ambito di indagini e/o accertamenti, al fine di dimostrare la rispondenza delle attività svolte ai requisiti normativi.