SEA – Segnaletica Stradale S.p.A.

Data Privacy Policy

approvata il 24 maggio 2018

SOMMARIO

1 PREMESSA

1.1 GLOSSARIO

Al fine di agevolare la comprensione delle tematiche riportate nella presente politica in materia di protezione dei dati personali (la "**Data Privacy Policy**"), di seguito vengono riportate le definizioni dei termini principali oggetto della stessa o alla quale essa richiama.

- **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 un interessato;
- **interessato**: una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **dati identificativi**: dati che permettono l'identificazione diretta, come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc;
- **dati sensibili**: quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;
- **dati giudiziari**: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- **pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **titolare del trattamento o Titolare**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- **responsabile del trattamento o Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un Titolare;
- **Garante**: l'Autorità Garante per la Protezione dei Dati personali;
- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- **terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **consenso dell'interessato** o **consenso:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **violazione dei dati personali** o **data breach:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **trattamento transfrontaliero**: *(i)* trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione Europea ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure *(ii)* trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione Europea, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- **GDPR**: 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;
- **Normativa Data Privacy:** il GDPR e ogni altro provvedimento in tema di protezione dei dati personali emanato dall'Unione Europea o dall'Italia, ivi inclusi i provvedimenti del Garante;
- **registro dei trattamenti**: il registro delle attività di trattamento di cui all'art. 30 del GDPR.
- **DPIA** o **Data Protection Impact Assessment**: la valutazione d'impatto dei trattamenti sulla protezione dei dati personali effettuata dal Titolare ai sensi dell'art. 35 del GDPR.

1.2 OBIETTIVO DEL DOCUMENTO E AMBITO DI APPLICAZIONE

La presente Data Privacy Policy si applica a SEA – Segnaletica Stradale S.p.A. (la "**Società**"), con particolare riferimento ai trattamenti di dati personali da quest'ultima effettuati tramite i propri dipendenti, collaboratori o soggetti comunque autorizzati (persone fisiche e giuridiche) allo svolgimento di attività di trattamento.

La tutela dei dati personali rappresenta un valore di fondamentale importanza, da tenere in considerazione durante le attività svolte dalla Società. La Società intende prestare la massima attenzione alla tutela dei dati personali, tenendo anche conto delle nuove vulnerabilità e minacce che insistono sui dati personali. Questo nuovo contesto richiede pertanto una più attenta gestione del dato personale in tutte le fasi di trattamento, dalla raccolta sino alla fase di dismissione (cancellazione e/o anonimizzazione dei dati).

In particolare, la Società si trova a dover gestire:

- diversi canali di acquisizione dei dati;
- diverse tipologie di dati personali;
- diverse categorie di interessati.

Al fine di garantire una gestione della data protection conforme alla Normativa Data Privacy, la Società ha predisposto e adottato la presente Data Privacy Policy, la quale si articola nelle seguenti sezioni:

- **Sezione I "Premessa"**: descrive gli obiettivi della presente Data Privacy Policy;
- **Sezione II "Governance"**: "descrive chiaramente i ruoli e le responsabilità data protection dei soggetti coinvolti nel trattamento dei dati personali, nonché le strutture organizzative della Società che a vario titolo possono essere coinvolte nella tutela dei dati personali;
- **Sezione III "Modello di Gestione Data Protection"**: descrive il Modello di Gestione Data Protection ovvero il modello operativo da utilizzare per gestire il dato personale in tutte le sue fasi del ciclo di vita (dalla raccolta fino alla cessazione/cancellazione del trattamento);
- **Sezione IV "Esercizio diritti degli interessati"**: descrive le modalità per l'esercizio di tutti i diritti da parte degli interessati (accesso, cancellazione-oblio, limitazione del trattamento, opposizione, portabilità), nonché i principali obblighi in capo alla Società in questo ambito;
- **Sezione V "Data Breach":** descrive le principali prescrizioni GDPR in materia di data breach;
- **Sezione VI "Domini di gestione in Data Protection"**: descrive le principali prescrizioni e adempimenti in materia di privacy by design e by default, autorizzazione e autenticazione, anonimizzazione e pseudonimizzazione, data retention, trasferimenti di dati extra UE;
- **Sezione VII "Ispezioni da parte del Garante e Sanzioni"**: descrive ruoli e responsabilità in caso di ispezioni da parte del Garante e di altre autorità di vigilanza, nonché le sanzioni in caso di violazione della Normativa Data Privacy;
- **Sezione VIII "Formazione"**: descrive gli elementi essenziali della formazione data protection, nonché la periodicità con cui deve essere svolta;
- **Sezione IX "Audit"**: descrive le attività di verifica che possono essere svolte dalla Funzione di Audit, al fine di verificare lo stato di conformità rispetto alla Normativa Data Privacy.

1.3 APPROVAZIONE E AGGIORNAMENTO DEL DOCUMENTO

La presente Data Privacy Policy è approvata ed emanata dall'Amministratore Delegato della Società. L'entrata in vigore è da intendersi immediatamente successiva alla sua approvazione.

L'Amministratore Delegato valuta, con cadenza annuale, se procedere ad una revisione della presente Data Privacy Policy, tenendo conto tra l'altro, dell'efficacia dimostrata nella prassi applicativa e di eventuali modifiche intervenute nella normativa di riferimento (le variazioni normative che non richiedono un processo di valutazione e decisione per il recepimento trovano applicazione dalla data di entrata in vigore delle medesime; il formale recepimento nella Data Privacy Policy è effettuato nella prima revisione utile).

2 GOVERNANCE

2.1 RUOLI, FUNZIONI E RESPONSABILITÀ

2.1.1 TITOLARE DEL TRATTAMENTO

La Società è identificata quale Titolare.

Pertanto, ogni riferimento nella presente Data Privacy Policy al Titolare va inteso alla Società e, funzionalmente, all'Amministratore Delegato della stessa, al quale sono conferiti i poteri decisionali e gestionali in materia di protezione dei dati personali.

Di seguito si riportano alcune tra le principali decisioni adottate dal Titolare:

- la tipologia di dati personali da raccogliere;
- le modalità e i sistemi utilizzati per il trattamento dei dati personali;
- le finalità del trattamento dei dati;

- la necessità di trasferire o meno i dati a terzi;
- le modalità e il periodo di conservazione dei dati personali;
- le misure tecniche e organizzative da adottare per la protezione dei dati personali
- ruoli e responsabilità all'interno del modello organizzativo data privacy.

2.1.2 DATA MANAGER

Il Titolare può nominare, sulla base della propria complessità organizzativa, uno o più "data manager", identificati nelle persone fisiche preposte alla conduzione delle strutture organizzative aziendali di particolare rilevanza rispetto al trattamento dei dati personali ("**Data Manager**").

Il Data Manager ha il compito di supervisionare, anche sulla base delle istruzioni impartitegli dalla Società (in qualità di Titolare o Responsabile del trattamento), lo svolgimento delle operazioni di trattamento che vengono effettuate dagli Incaricati che operano nell'ambito della struttura organizzativa di cui è responsabile.

Si indicano qui di seguito le principali ambiti di intervento del Data Manager:

- collaborare con il Titolare, il Referente Data Protection e gli altri Data Manager nell'esecuzione degli adempimenti previsti dalla Normativa Data Privacy;
- procedere all'identificazione degli Incaricati per la propria area di competenza, fornendo ai medesimi istruzioni scritte e dettagliate circa le modalità del trattamento, ove tali istruzioni non siano state precedentemente fissate da parte del Titolare, anche a mezzo di ordine di servizio;
- fornire al Titolare, su richiesta di quest'ultimo, la mappatura aggiornata degli Incaricati e delle istruzioni loro impartite;
- monitorare le operazioni di trattamento svolte dai propri Incaricati e verificare che vengano eseguite in conformità alle istruzioni agli stessi impartite e solo relativamente agli ambiti di trattamento loro consentiti;
- verificare il rispetto dei requisiti di liceità e correttezza del trattamento sui dati personali effettuato da terzi nell'ambito della propria area di competenza;
- monitorare l'applicazione dei processi previsti al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- gestire - tramite adeguate procedure, secondo criteri di efficienza - la documentazione relativa agli adempimenti documentali prescritti dalla Normativa Data Privacy, garantendone la custodia, la non alterazione ed il pronto ritrovamento;
- monitorare l'applicazione di adeguate misure tecniche e organizzative che garantiscano un adeguato livello di protezione dei dati personali trattati nella propria area di appartenenza;
- assicurare che l'informativa di cui agli artt. 13 e 14 del GDPR sia inoltrata a tutti gli interessati;
- verificare il rispetto dei tempi di conservazione, ponendo la necessaria attenzione alle attività volte alla cancellazione dei dati personali e garantendo che queste siano conformi alle prescrizioni della Normativa Data Privacy;
- garantire l'aggiornamento della mappatura dei dati personali trattati nella struttura organizzativa di propria competenza, supportando il Referente Data Protection nella tenuta e aggiornamento del registro trattamenti;
- supportare il Referente Data Protection nell'esecuzione della DPIA;
- garantire l'applicazione del principio di privacy by design e by default;

- qualora il trattamento di dati personali rientranti nella propria area di competenza preveda la trasmissione di dati fuori dai confini dell'Unione Europea, verificare se il paese destinatario rientri fra quelli considerati dalla Commissione Europea come provvisti di un sistema di protezione dei dati personali adeguato rispetto alla protezione accordata dal GDPR; in caso contrario, accertare che la trasmissione sia legittimata dal ricorso a misure di salvaguardia come, ad esempio, l'utilizzo dei modelli di clausole contrattuali standard ("SCC") approvati dalla Commissione UE.

Ciascun Data Manager viene nominato ed opera sulla base delle istruzioni stabilite dal Titolare.

2.1.3 REFERENTE DATA PROTECTION

Il Titolare può identificare all'interno del Gruppo Data Manager un responsabile dello sviluppo del modello di gestione dei dati personali (il "**Referente Data Protection**").

Il Referente Data Protection agisce quale coordinatore del Gruppo Data Manager e dell'impianto di gestione dei dati personali, monitorando l'attuazione della presente Data Privacy Policy e delle altre procedure sulla protezione dei dati personali adottate dalla Società.

In particolare, il Referente Data Protection:

- coordina l'esecuzione delle attività previste dal modello di gestione data protection implementato dalla Società;
- coordina le attività del Gruppo Data Manager e ne presiede le riunioni;
- informa il Titolare di eventuali temi rilevanti emersi e sviluppati all'interno del Gruppo Data Manager;
- cura la tenuta e l'aggiornamento del registro dei trattamenti sulla base del censimento effettuato dai Data Manager relativamente alle rispettive area di competenza,
- collabora con la Funzione Legale e Compliance nella definizione e aggiornamento della documentazione in ambito data protection;
- con particolare attenzione al processo di rilevazione delle violazioni (data breach), coopera nelle attività di notifica al Garante, e se del caso all'interessato, ed alle successive attività prescritte della normativa (artt. 33 e 34 del GDPR).

2.1.4 SUBDELEGATI

Ove ritenuto opportuno in ragione della complessità dell'area aziendale di competenza, il Data Manager potrà nominare uno o più subdelegati, che agiscano in sua vece nelle operazioni data protection (i "**Subdelegati**").

I Subdelegati hanno il compito di supportare operativamente il Data Manager nell'attuazione dei compiti affidatigli e di garantire l'affidabile ed agevole implementazione delle conseguenti azioni esecutive.

Tra i compiti dei Subdelegati vi sono:

- relazionarsi con gli incaricati dell'area di pertinenza, fornendo loro istruzioni di dettaglio nello svolgimento delle proprie mansioni che coinvolgano operazioni di trattamento di dati personali;
- verificare il rispetto da parte degli incaricati delle istruzioni loro impartite, comunicando tempestivamente al Data Manager eventuali situazioni di disallineamento o di rischio per gli interessati;
- provvedere al censimento dei trattamenti operati nell'area di competenza, evidenziando eventuali carenze informative e, in tal caso, comunicarle al Data Manager;

- nell'ambito delle relazioni con terze parti intrattenute dalla area di competenza, verificare preliminarmente gli impatti in termini di protezione dei dati personali al fine di appurare la necessità di contrattualizzare l'eventuale rapporto con la terza parte in qualità di Responsabile, con la conseguente applicazione delle clausole contrattuali standard;
- qualora dovesse venire a conoscenza di casi di violazione di dati personali, fornire la tempestiva comunicazione al Data Manager, che a sua volta informerà il Referente Data Protection.

2.1.5 INCARICATI AL TRATTAMENTO

Gli incaricati sono tutti i soggetti autorizzati dal Titolare o dal Data Manager al trattamento di dati personali, secondo specifiche e formali direttive impartite dai medesimi (gli "**Incaricati**"). È presumibile che tutti i dipendenti del Titolare debbano essere inquadrati come Incaricati e quest'ultimi devono trattare i dati personali solo ove ciò risulti strettamente necessario per l'esercizio delle proprie mansioni.

2.1.6 AMMINISTRATORI DI SISTEMA

Il Titolare nomina uno o più amministratori di sistema preposti alla gestione di sistemi informatici con i quali vengono effettuati trattamenti di dati personali (gli "**Amministratore di Sistema**").

La particolare capacità di azione propria dell'Amministratore di Sistema e la natura fiduciaria delle relative mansioni rappresentano, quindi, elementi fondanti del ruolo, atteso che l'Amministratore di Sistema può:

- può accedere, potenzialmente, a tutti i dati personali, e più in generale alle informazioni che sono elaborate dal sistema informativo aziendale;
- gestire utenze e profilazioni;
- eventuali altre attività ritenute critiche in materia data protection e sicurezza informatica.

A titolo esemplificativo sono considerati Amministratore di Sistema i soggetti che svolgono attività riconducibili alle mansioni di:

- amministratore di sistema operativo;
- amministratore di database;
- amministratore di sistemi software complessi quali a titolo esemplificativo e non esaustivo sistemi ERP (Enterprise resource planning), sistemi CRM etc;
- amministratore di rete;
- amministratore di sistemi di sicurezza.

Ciascun Amministratore di Sistema opera sulla base delle istruzioni stabilite dal Titolare.

Qualora siano nominati più Amministratori di Sistema, questi si riuniscono, almeno annualmente, al fine di sviluppare un confronto ed il coordinamento sulle tematiche operative e tecniche affrontate nelle rispettive aree di competenza.

2.1.7 FUNZIONE LEGALE E COMPLIANCE

La Funzione Legale e Compliance supporta il Titolare, il Referente Data Protection, i Data Manager e le altre funzioni aziendali competenti nella ricognizione ad applicazione della Normativa Data Privacy. Inoltre, la Funzione Legale e Compliance:

- predispone e aggiorna i modelli della documentazione ai sensi della Normativa Data Privacy (quali lettere di nomina e istruzioni, informative e relativi consensi).

- predispone e aggiorna, con il supporto della Funzione Acquisti, le clausole contrattuali data protection standard da adottare con fornitori e terze parti.
- fornisce supporto nella gestione di eventuali controversie (ricorsi dell'interessato, contestazioni del Garante, ecc.).

2.1.8 FUNZIONE IT

La Funzione IT ha il compito di definire ed implementare le misure di sicurezza che dovranno essere implementate per garantire la sicurezza del trattamento di dati personali, nonché monitorare le attività in essere al fine di individuare anomalie di sicurezza che potrebbero comportare una violazione dei dati personali.

La Funzione IT ha i seguenti ambiti di intervento:

- implementare i requisiti di sicurezza relativi alle credenziali di autenticazione degli incaricati al trattamento;
- definire, in caso di implementazione di nuovi sistemi/servizi informativi o la modifica di quelli esistenti, nell'ottica privacy by design e by default i requisiti di riservatezza e protezione dei dati personali;
- fornire supporto alle diverse unità organizzative che trattano dati personali, tramite l'utilizzo dei sistemi informativi aziendali anche con riferimento all' individuazione delle idonee misure di sicurezza;
- monitorare l'implementazione delle misure di sicurezza definite per i sistemi informativi della Società, al fine di garantire la tempestiva rilevazione di eventuali data breach;
- in caso di violazione di dati personali, prestare la necessaria collaborazione al Titolare, al Referente Data Protection ed ai Data Manager, per l'individuazione delle opportune contromisure da adottare;
- definire misure di sicurezza logiche per l'accesso alle basi dati elettroniche e adeguate misure di sicurezza fisiche per l'accesso ai locali adibiti a data center;
- gestire incidenti di sicurezza informatica relativi ai dati personali in conformità alla Normativa Data Privacy, alla presente Data Privacy Policy e alle ulteriori procedure adottate dalla Società;
- supportare il Titolare nell'identificazione degli Amministratori di Sistema;
- confrontarsi periodicamente con gli Amministratori di Sistema;
- garantire, nel rispetto della Normativa Data Privacy, la raccolta e il monitoraggio dei log relativi alle attività degli Amministratori di Sistema (login, logout), fornendo il proprio supporto alle competenti strutture organizzative nelle attività di verifica periodica.

2.1.9 FUNZIONE RISORSE UMANE

La Funzione Risorse Umane ha il compito di supportare i processi di gestione dei dati personali dei dipendenti e dei candidati e di supportare la diffusione della cultura data protection tra i dipendenti della Società. In particolare, la Funzione Risorse Umane supporta il Titolare e il Referente Data Protection *(i)* nell'individuazione del personale (dipendenti e collaboratori) autorizzato al trattamento dei dati personali; *(ii)* nella fornitura ai dipendenti del materiale formativo sulla data privacy e nell'organizzazione di corsi per l'approfondimento delle tematiche data protection definite.

2.1.10 FUNZIONE ACQUISTI

La Funzione Acquisti ha il compito di gestire i rapporti con i fornitori che trattano dati personali per conto della Società, che possono essere nominati quali Responsabili del trattamento.

La Funzione Acquisti svolge le seguenti attività:

- gestisce, con il supporto della Funzione Legale e Compliance, il processo di nomina dei Responsabili del trattamento, su indicazione delle strutture organizzative richiedenti che identificano i fornitori che trattano dati personali per conto della Società;
- gestisce e conserva il contratto di fornitura, nonché l'atto di nomina a Responsabile trattamento;
- supporta la Funzione Legale e Compliance nella definizione e aggiornamento delle clausole data protection da inserire nel contratto di fornitura.

2.1.11 FUNZIONI DI BUSINESS

Tutte le Funzioni di Business hanno l'obbligo di rispettare i principi di privacy by design e by default e supportare il Titolare e il Data Manager nell'attività di aggiornamento del registro dei trattamenti.

3 MODELLO DI GESTIONE DATA PROTECTION

Nell'ambito delle operazioni di trattamento svolte, la Società, anche attraverso i propri Data Manager, dovrà porre in essere tutte le misure necessarie per tutelare i dati personali, dovendo garantire:

- la confidenzialità, integrità e disponibilità dei dati personali trattati;
- il test e la valutazione periodica di efficacia delle procedure e delle misure implementate;
- l'implementazione di misure di protezione delle reti, dei sistemi e dei software con i quali vengono trattati i dati personali, quali ad esempio:
    - la pseudonimizzazione, l'offuscamento e la cifratura dei dati personali;
    - soluzioni di continuità di servizio in grado di garantire la disponibilità e l'integrità dei dati (backup, disaster recovery, ecc.).
- la definizione di clausole contrattuali finalizzate a vincolare le terze parti al rispetto delle eventuali misure di sicurezza aggiuntive richieste dalla Società;
- la definizione di adeguate informative e consensi che garantiscano la trasparenza del trattamento;
- l'adozione di una metodologia di DPIA, in grado di garantire l'identificazione e minimizzazione dei rischi che possono insistere sui dati personali derivanti da nuovi progetti e prodotti;
- l'applicazione del principio di data protection by design e by default nella progettazione dei sistemi e nel disegno dei processi e delle procedure aziendali;
- l'implementazione di soluzioni in grado di rilevare tentativi non leciti di accesso ai dati personali in grado di garantire il rispetto delle prescrizioni del GDPR in merito alle violazioni (data breach).

Pertanto, al fine di gestire il dato personale in tutte le sue fasi del ciclo di vita (dalla raccolta fino alla cessazione/cancellazione del trattamento), la Società ha definito un Modello di Gestione Data Protection, il quale si suddivide in 3 macrofasi, ciascuna con degli obiettivi specifici di seguito riportati:

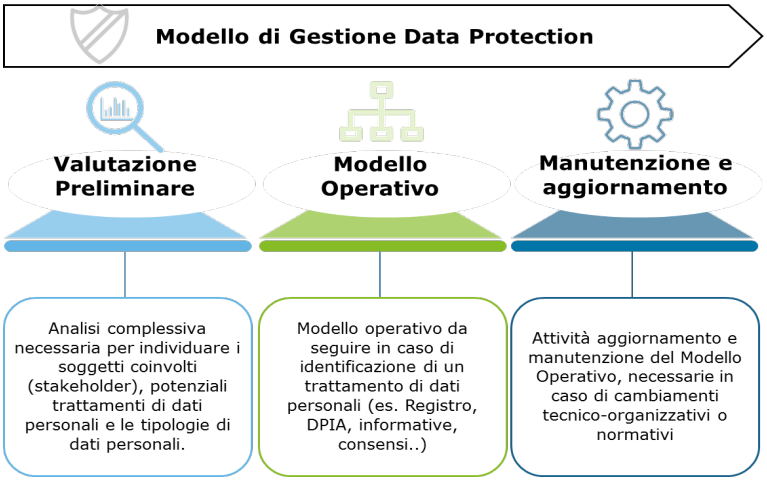


Figure 1: Modello di Gestione Data Protection

- **Fase 1 - Valutazione preliminare:** l'obiettivo di questa fase è di effettuare una prima analisi complessiva della progettualità (processo/attività/prodotto) al fine di individuare i soggetti coinvolti (stakeholder), potenziali trattamenti di dati personali e le tipologie di dati personali;
- **Fase 2 - Modello operativo:** l'obiettivo di questa fase è di fornire delle indicazioni sulle attività che devono essere svolte con riferimento al trattamento identificato. In particolare è stato definito un Modello operativo, il quale è costituito dalle seguenti fasi:
    1. Valutazione proporzionalità e necessità del trattamento
    2. Registro dei trattamenti
    3. DPIA
    4. Informative
    5. Consensi
    6. Terze parti e Clausole contrattuali
    7. Misure by Design
- **Fase 3 - Manutenzione e aggiornamento:** in questa fase vengono descritte le attività di aggiornamento e manutenzione del Modello Operativo, necessarie in caso di cambiamenti tecnico-organizzativi o normativi.

Con riferimento ai ruoli e le responsabilità del Modello di Gestione Data Protection, per ciascuna delle attività previste all'interno dello stesso è stata predisposta una Matrice RACI che individua il ruolo di ciascuno degli stakeholder coinvolti. In particolare sono stati individuati i seguenti ruoli e responsabilità:

- **Responsible (R)**
    - Esegue/Coordina il processo di predisposizione delle informazioni;
    - Spiega/supporta le informazioni di input/output sui singoli task al fine di consentire alla Funzione «Accountable» di apporre il sign off;

- Si tratta del responsabile operativo per la correttezza e il completamento dell'attività;
- Viene coinvolto in caso risultino necessari chiarimenti sulle informazioni censite.

- **Accountable (A)**
  - Responsabile ultimo (approvatore) della correttezza e del completamento dell'attività.
- **Consulted (C)**
  - Esprime punti di vista basati su esperienza/opinioni e dà il suo contributo;
  - Soggetto che deve essere coinvolto in quanto possiede le informazioni rilevanti e le competenze necessarie per il completamento del progetto e delle attività.
- **Informed (I)**
  - Invia/riceve informazioni riguardo alle attività ed al loro stato di completamento.

3.1 VALUTAZIONE PRELIMINARE

La presente macrofase prevede l'analisi complessiva della progettualità (processo/attività/prodotto) al fine di individuare i soggetti coinvolti (stakeholder), potenziali trattamenti di dati personali e le tipologie di dati personali. Tale macrofase è composta dalle seguenti attività:

- **Analisi degli stakeholder:** individua i soggetti (stakeholder) cui è rimessa la primaria identificazione se il progetto/prodotto prevede un trattamento di dati personali. In particolare gli stakeholder coinvolti possono essere:
  - **Incaricato:** l'Incaricato del trattamento che ha avviato/sta avviando la nuova progettualità che potrebbe comportare un nuovo trattamento e che prevede il coinvolgimento di dati personali;
  - **Data Manager:** il Data Manager, identificato responsabile di funzione, dell'area in cui lavora l'Incaricato del trattamento, e che verrà coinvolto da questi per un preliminare confronto sulla progettualità;
  - **Referente Data Protection:** deve essere coinvolto in ogni fase della presente Data Privacy Policy;
  - **Funzione Legale e Compliance:** in base al progetto/trattamento, ha il compito di fornire un supporto normativo e privacy, sia nella primaria identificazione della presenza o meno di dati personali che nei successivi steps di natura organizzativo-normativa (proporzionalità e necessità del trattamento, DPIA, informative e consensi.);
  - **Funzione IT:** la Funzione IT, in base al progetto/trattamento, potrà essere coinvolta nelle fasi più tecniche quali DPIA, Misure by design, Sicurezza del Codice;
  - **Funzione Acquisti:** potrà essere coinvolto nel caso in cui debba essere ingaggiato un nuovo fornitore/modificate le clausole contrattuali in essere.
- **Identificazione delle PII:** prevede l'identificazione da parte degli stakeholder coinvolti delle tipologie di informazioni personali identificabili (PII), ossia quelle da cui possono essere ricavati dei dati personali, che potrebbero essere trattate nell'ambito del nuovo trattamento/progetto.

Se l'esito dell'identificazione di PII:

- **è negativo**: verrà documentata l'assenza di PII e il progetto potrà proseguire senza l'applicazione dei successivi steps della presente Data Privacy Policy;
- **è positivo**: sarà necessario procedere con le successive valutazioni e pertanto si applicherà integralmente la presente Data Privacy Policy.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di valutazione preliminare.

Strutture organizzative / *Attività*	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 1: Valutazione Preliminare						
Analisi degli stakeholder	R	R/A	C	C	C	C
Identificazione delle PII	R	R/A	C	C	C	C

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.1.1 MODELLO OPERATIVO DI DATA PROTECTION

Terminata la fase di valutazione preliminare, necessaria per identificare la presenza o meno di dati personali, con riferimento al trattamento identificato, devono essere intraprese le opportune azioni, volte a garantire una adeguata gestione del trattamento stesso.

In particolare sono state previste le seguenti attività:

- **valutazione proporzionalità e necessità del trattamento:** valutazione che deve essere svolta per ogni trattamento di dati personali per stabilire se lo stesso è necessario e proporzionato rispetto alle finalità;
- **registro dei trattamenti:** attività di censimento del trattamento identificato sulla base dei requirements previsti dall'art. 30 del GDPR;
- **DPIA:** attività di valutazione dell'impatto del trattamento sui dati personali con riferimento ai diritti e alla libertà degli interessati;
- **informative:** l'informativa rappresenta la principale forma di trasparenza nei confronti degli interessati, pertanto dovrà essere concisa, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro;
- **consensi**: il consenso costituisce uno dei requisiti di legittimità al trattamento dei dati personali degli interessati, pertanto deve essere presentato in modo chiaramente distinguibile, deve essere facilmente accessibile, libero, specifico, informato, inequivocabile e deve essere reso attraverso dichiarazione scritta o azione positiva anche attraverso mezzi elettronici o orali;
- **terze parti e clausole contrattuali**: nel caso in cui un trattamento è affidato ad un soggetto esterno è necessario provvedere alla nomina dello stesso quale responsabile del trattamento e dovranno essere previste specifiche clausole data protection;

- **misure by design**: ciascun trattamento di dati personali dovrà prevedere idonee misure tecniche di sicurezza, tenendo in considerazione le finalità del trattamento, il contesto e la natura dei dati trattati.

3.1.2 PROPORZIONALITÀ E NECESSITÀ DEL TRATTAMENTO

Il principio di "proporzionalità e necessità del trattamento" ispira tutto il GDPR, e rappresenta il punto di partenza di ogni valutazione circa un nuovo trattamento di dati personali.

A tal fine, si rende necessario valutare le misure da introdurre/adeguare nel trattamento (legate all'implementazione/ adeguamento di un progetto/ processo/attività/prodotto) che contribuiscono:

- alla proporzionalità e necessità del trattamento;
- al soddisfacimento dei diritti degli interessati.

In particolare dovranno essere verificati e valutati i seguenti aspetti:

- **Finalità specifiche, esplicite e legittime:** i dati personali devono essere raccolti soltanto per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Pertanto, nell'ambito del trattamento i dati dovranno essere raccolti per le specifiche finalità di cui all'informativa;
- **Liceità del trattamento:** ai sensi dell'art. 6 del GDPR, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
  - l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
  - il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
  - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
  - il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
  - il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
  - il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, 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. Nell'ambito del nuovo trattamento/progetto dovrà pertanto essere chiaramente individuata la base (o le basi) che ne giustificano la liceità.
- **Dati adeguati, pertinenti, esatti e limitati a quanto necessario:** nel rispetto del principio di c.d. "data minimization" (minimizzazione dei dati) di cui all'art. 5(1) lettera c) e d) GDPR, i dati richiesti agli interessati dovranno essere limitati a quanto necessario rispetto alle finalità perseguite dal trattamento;
- **Periodo limitato di conservazione:** i dati dovranno essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali vengono trattati. Tale periodo dovrà essere determinato sulla base di quanto prevista nel paragrafo 6.3 Data Retention cui si rimanda;

- **Diritti degli interessati:** con riferimento all'esercizio dei diritti degli interessati di cui al GDPR (Diritto di accesso, diritto di portabilità, diritto di opposizione, diritto di revoca del consenso, diritto di rettifica, diritto di limitazione, diritto di cancellazione) si rimanda al capitolo 4 Esercizio diritti degli interessati.

3.1.3 REGISTRO DEI TRATTAMENTI

Una volta confermata la necessità e la proporzionalità del trattamento, ai sensi dell'art.30 del GDPR è necessario censire il trattamento all'interno del registro dei trattamenti. Secondo quanto previsto dall'art. 30 del GDPR, il registro dei trattamenti dovrà contenere le seguenti informazioni:

- **Titolare del trattamento (o Rappresentante del Titolare del Trattamento);**
- **Struttura Organizzativa**: struttura organizzativa della Società di riferimento che utilizza i dati personali per lo svolgimento delle sue attività lavorative compresa l'indicazione del soggetto da identificare come Data Manager;
- **Finalità del trattamento:** scopo della raccolta dei dati e descrizione dettagliata della finalità e dell'impiego del dato;
- **Dato Personale:** indicazione della tipologia di dato trattato:
  - Comune;
  - Sensibile;
  - Giudiziario.
- **Categoria dell'Interessato:** macro classificazione dell'interessato (es. cliente, dipendente, intermediario, candidato, familiare, soggetto terzo, fornitore ecc.);
- **Periodo di conservazione:** periodo di retention dei dati stabilito;
- **Categorie di destinatari UE ed Extra UE:**
  - categoria del destinatario (es. riassicuratori);
  - destinatario del trasferimento (nome dell'entità giuridica che tratta/riceve i dati);
  - ruolo del destinatario (Responsabile, Titolare o Organizzazione Internazionale);
  - posizione fisica (UE o extra UE);
  - base giuridica (selezionare la base giuridica che permette il trasferimento extra UE nel rispetto delle normative quali ad esempio consenso, Privay Shield, BCR, Data Protection Agreement, Model Contract Clauses, Certificazioni).
- **Strumenti utilizzati per il trattamento:**
  - Applicativi / database in cui sono immagazzinati i dati;
  - Archivi fisici dove viene conservata la documentazione inerente il trattamento.
- **Descrizione delle Misure di sicurezza adottate:** generale descrizione delle misure di sicurezza tecniche ed organizzative messe in atto o da attuare, in conformità con l'art. 32.1 del GDPR;
- **Strutture che concorrono al trattamento:** strutture organizzative interne ed esterne alla Compagnia coinvolte nell'utilizzo o nel trattamento dei dati personali per lo svolgimento delle attività lavorative.

Il registro dei trattamenti, affinché possa considerarsi uno strumento utile per disporre di un quadro aggiornato dei trattamenti svolti dalla Società ed indispensabile per ogni valutazione e analisi del rischio, dovrà essere mantenuto aggiornamento con cadenza almeno annuale.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di predisposizione del registro dei trattamenti.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 2: Modello Operativo						
Registro dei trattamenti	-	R	R/A	C	I	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.1.4 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Quando un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà degli interessati, la Società esegue, prima di procedere al trattamento, una valutazione dell'impatto del trattamento sui dati personali, con particolare riguardo al loro diritto alla protezione dei dati personali.
Tale valutazione deve essere eseguita in tutti i casi nei quali una prima analisi nota come "Valutazione preliminare rischio privacy" porti a ritenere che il trattamento presenti dei rischi specifici in base alla tipologia dei dati trattati, alle caratteristiche ed alle modalità del trattamento, agli strumenti utilizzati ed alle possibili ricadute sui diritti e le libertà degli interessati. In questo caso si procederà con lo svolgimento di una DPIA, in linea con la "Metodologia di analisi dei rischi data protection e di valutazione degli impatti" adottata dalla Società, cui si rimanda.
La valutazione d'impatto è, comunque, eseguita nei seguenti casi:

- trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni automatizzate che hanno effetti giuridici o incidono in modo analogo significativamente sugli interessati;
- il trattamento, su larga scala, di dati particolari che presentano un elevato rischio ai diritti e alla libertà degli interessati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- trattamento di dati soggetti a valutazione d'impatto richiesti dal Garante tramite elenchi resi pubblici dalla stessa autorità;

Nel dettaglio, tale valutazione d'impatto sulla protezione dei dati comprende:

- una descrizione chiara ed esaustiva dei trattamenti previsti, delle finalità del trattamento e, se del caso, degli interessi legittimi perseguiti dal Titolare del trattamento che dovranno essere non inferiori ai diritti ed alle libertà fondamentali dell'interessato;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- un elenco delle garanzie, delle misure di sicurezza e dei meccanismi per garantire la protezione dei dati personali che il Titolare valuta necessario adottare al fine di dimostrare la conformità del trattamento, tenuto conto dei diritti e dei legittimi interessi degli interessati e delle altre persone in questione, alle prescrizioni della normativa in materia di protezione dei dati.

All'esito della DPIA (qualora necessaria) verranno indicate le misure previste per mitigare i rischi e, qualora il trattamento possa presentare un rischio ancora elevato, si procederà a consultare preventivamente l'Autorità Garante ai sensi dell'art. 26 GDPR.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di DPIA.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 2: Modello Operativo						
DPIA	I	R	R/A	C	C	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.1.5 INFORMATIVE

I dati personali devono essere trattati in modo lecito, corretto e trasparente. Il principale strumento offerto ai Titolari del trattamento per dimostrare la propria trasparenza nei confronti degli interessati è rappresentato dall'informativa privacy, che deve essere concisa, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro.

L'informativa relativa al trattamento dei dati personali dell'interessato è strutturata indicando almeno i seguenti elementi:

- gli estremi identificativi del Titolare del trattamento e le relative modalità di contatto;
- le finalità del trattamento;
- la base giuridica sulla quale poggia il trattamento qualora esso si basi sul principio del "legittimo interesse";
- le categorie dei dati personali;
- l'obbligatorietà o meno del conferimento dei dati personali e le conseguenze di un eventuale rifiuto;
- la possibilità di trasferimento in Paesi situati al di fuori dell'Unione Europea, qualora applicabile;
- l'identificazione dei destinatari o le eventuali categorie dei destinatari;
- il periodo di conservazione oppure i criteri utilizzati per determinarlo;

- i dati di contatto del responsabile della protezione dei dati (al fine di esercitare i propri diritti);
- l'esistenza dei diritti riconosciuti all'interessato;
- il diritto di proporre reclamo all'Autorità di controllo;
- l'esistenza di un (eventuale) processo decisionale automatizzato, compresa la profilazione, le logiche applicate e le conseguenze per l'interessato;
- la fonte dalla quale sono acquisiti i dati nel caso in cui non siano forniti direttamente dall'interessato.

L'informativa deve essere sempre fornita all'interessato al momento della raccolta dei dati personali o, al più tardi, entro un mese dall'acquisizione se avvenuta presso terzi, ed in particolare nei casi di seguito specificati (elencazione non esaustiva):

- selezione e assunzione di dipendenti (incluse tutte le forme di collaborazione in uso);
- offerta di prodotti e servizi;
- impiego di siti web per la proposizione dell'offerta commerciale nel caso in cui attraverso il sito internet venga richiesto di fornire o vengano raccolti dati personali (es. utilizzando i cookies);
- utilizzo di sistemi di videosorveglianza e, più in generale, in occasione del controllo accessi presso sedi della Società;
- partecipazioni ad iniziative ed eventi.

In fase di avvio della raccolta di dati personali è pertanto necessario adottare un'adeguata informativa.

Al fine di rispettare i requirement del GDPR e le best practices in materia di data protection, la Società ha definito nuove informative che rispecchiano i requisiti stabili dagli artt. 13 – 14 del GDPR.

Nel caso in cui i dati personali debbano essere utilizzati per finalità diverse da quelle espresse nell' informativa, le relative operazioni di trattamento non potranno essere svolte fino a quando gli interessati non siano stati adeguatamente informati. In questo caso sarà necessario procedere alla redazione di una nuova informativa/integrazione di quelle esistenti, in linea con quanto previsto dagli artt. 13 e 14 del GDPR.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella predisposizione delle informative.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliace	IT	Acquisti
Fase 2: Modello Operativo						
Informative	R	R	R	R/A	C	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)

I: Informato (Informed)

3.1.6 CONSENSI

Il consenso costituisce uno dei requisiti di legittimità al trattamento dei dati personali degli interessati, tuttavia, per essere una base giuridica lecita, deve essere presentato in modo chiaramente distinguibile, deve essere facilmente accessibile, libero, specifico, informato, inequivocabile e deve essere reso attraverso dichiarazione scritta o azione positiva anche attraverso mezzi elettronici o orali. Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In fase di avvio di un nuovo progetto/ trattamento è necessario prevedere, oltre ad un'adeguata informativa anche adeguati moduli di consenso, laddove necessari.

Il consenso espresso dagli interessati non è, in ogni caso, necessario per lo svolgimento di operazioni di trattamento nei casi previsti dalla normativa[1].

Si citano qui di seguito, a mero titolo esemplificativo, alcune delle finalità per le quali è necessario raccogliere specifico consenso:

- attività di marketing;
- attività di profilazione;
- attività di analisi di mercato;
- attività concernenti il trattamento di dati particolari o (se non esistono altre basi legali previste dalla normativa).

Il consenso viene considerato valido qualora rispetti i seguenti requisiti:

- **Informato**: il consenso deve essere preceduto dalla consegna o, in ogni caso, dalla presa visione da parte dell'interessato dell'informativa;
- **Specifico**: deve essere oggetto di uno specifico consenso ciascuna operazione di trattamento che, in mancanza di un diverso presupposto di legittimità del trattamento, necessiti del consenso degli interessati;
- **Espresso**: l'intenzione dell'interessato di prestare il proprio consenso alle operazioni di trattamento che lo riguarderanno deve essere espressa tramite una chiara ed univoca manifestazione di volontà;
- **Libero**: l'interessato dovrà essere sempre messo in condizione di poter rifiutare di prestare il proprio consenso allo svolgimento di determinate operazioni di trattamento;
- **Esplicito**: l'avvenuta prestazione del consenso da parte di ciascun interessato potrà essere raccolta anche oralmente ma dovrà essere documentata. Per quanto riguarda il caso del trattamento di dati particolari, per i quali è necessaria una previa condizione di legittimità al loro trattamento, di norma è necessario il consenso "scritto" da parte dell'interessato, salvo che non ricorrano casi di esclusione (es. nel rapporto di lavoro, CV spontanei, ecc.).

[1] In alcuni casi, specificamente previsti dalla Normativa Data Privacy, il consenso dell'interessato non è necessario; nel rimandare al dettato normativo per la casistica completa, tra i predetti casi si evidenziano a titolo esemplificativo:
- l'adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o l'adempimento, prima della conclusione del contratto, di specifiche richieste dell'interessato stesso;
- l'acquisizione di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- il trattamento di dati relativi allo svolgimento di attività economiche (riferite all'interessato).

Gli interessati che abbiano prestato il consenso allo svolgimento di determinate operazioni di trattamento hanno sempre la facoltà di revocarlo successivamente, per motivazioni legittime. Nella suddetta ipotesi, le operazioni di trattamento svolte in virtù di tale consenso dovranno essere prontamente interrotte salvo che non ricorrano condizioni di "legittimo interesse" del Titolare che siano prevalenti rispetto agli interessi, ai diritti ed alle libertà fondamentali dell'interessato.

In caso di trattamento di dati personali è necessario prevedere, oltre ad un'adeguata informativa anche adeguati moduli di consenso, laddove necessari.

Al fine di rispettare i requirements del GDPR e le best practices in materia data protection, la Società ha definito nuovi moduli di consenso sulla base dei requisiti stabili dagli art. 4 del GDPR.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella predisposizione dei consensi.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	[Legale e Compliance	IT	Acquisti
Fase 2: Modello Operativo						
Consensi	R	R	R	R/A	I	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.1.7 TERZE PARTI E CLAUSOLE CONTRATTUALI

In fase di avvio di un nuovo progetto/trattamento si può rendere necessario l'affidamento di una parte dell'attività/ processo ad un soggetto esterno che erogherà il servizio in nome e per conto della Società. Al fine di valutare se vi sono possibili implicazioni dal punto di vista data protection, è necessario stabilire se l'attività del fornitore comporta un trattamento di dati personali e se è previsto un trasferimento di dati.

Per trattamento di dati personali effettuato da terze parti, si intendono tutte le casistiche in cui i dati personali di titolarità della Società siano resi, in qualsiasi modo, accessibili, anche tramite connessione remota, a terze parti.

In tale ipotesi, le terze parti devono essere nominate come Responsabili del trattamento, nel caso in cui effettuino i trattamenti sotto la direzione ed il controllo della Società. Nel caso in cui le terze parti agiscano quali Responsabili del trattamento, dovranno ricevere istruzioni scritte che specifichino almeno:

- l'obbligo di attenersi alle ulteriori istruzioni, di volta in volta, fornite dalla Società per assicurare la liceità delle operazioni di Trattamento;
- la garanzia che le persone autorizzate al trattamento si siano impegnate alla riservatezza;
- che sia implementato il processo per rispondere all'interessato nell'esercizio dei propri diritti, nell'eventualità che la Società abbia delegato al Responsabile del trattamento tale adempimento

ovvero che le richieste ricevute siano immediatamente trasferite alla Società affinché venga predisposto il necessario riscontro nel rispetto dei termini prescritti;

- l'obbligo di fornire tutte le informazioni necessarie per dimostrare il rispetto della Normativa Data Privacy e delle istruzioni ricevute fermo restando il diritto per la Società del di effettuare ispezioni relativamente alla corretta applicazione delle prescrizioni e delle istruzioni fornite;
- la necessità di predisporre ed aggiornare un registro dei trattamenti;
- l'obbligo di implementare adeguate misure di sicurezza tecniche ed organizzative per proteggere i dati personali;
- l'obbligo di nominare un Data Protection Officer, laddove richiesto;
- l'obbligo di adottare le salvaguardie di cui al paragrafo 6.4 Trasferimenti dati extra UE in caso di trasferimento di dati extra UE;
- l'obbligo di cessare immediatamente le operazioni di trattamento sui dati personali e provvedere alla loro cancellazione o renderli disponibili alla Società in caso di cessazione del rapporto di fornitura;
- l'obbligo di fornire una notifica immediata al titolare del trattamento in relazione a qualsiasi violazione dei dati personali o incidente che abbia impatto sui dati personali trattati per conto del titolare;
- l'obbligo di consentire eventuali audit da parte della Società e di prestare la più ampia collaborazione nella rilevazione di incidenti di sicurezza che interessino di dati personali (data breach) al fine di dare attuazione alle prescrizioni normative applicabili;
- l'obbligo, in caso di ricorso a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto della Società, di imporre mediante un contratto gli stessi obblighi in materia di protezione dei dati definiti nel contratto tra il titolare e la terza parte.

Di seguito viene riportato il workflow da tenere in considerazione nella gestione dei rapporti con le terze parti:

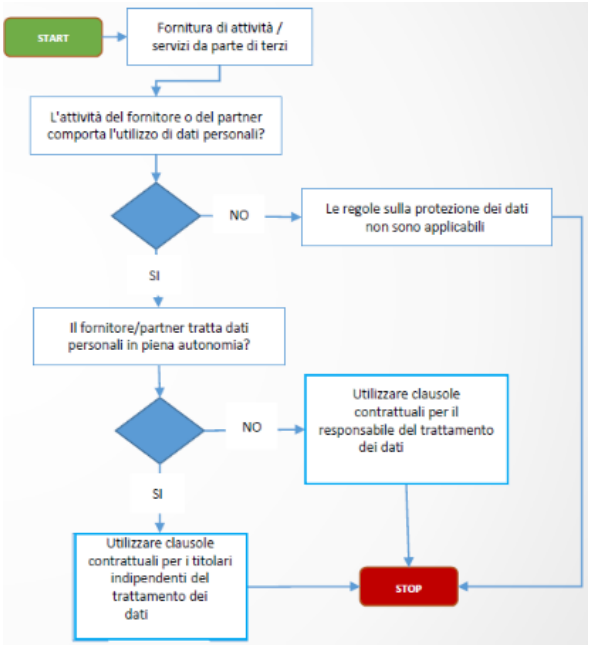


Figure 2: Workflow Rapporto con le Terze Parti

Nell'ambito di servizi che comportano il trattamento e il trasferimento di dati personali ai fornitori, la Società deve valutare l'autonomia di questi ultimi ai fini della definizione del suo ruolo e della sottoscrizione di uno dei seguenti accordi:

a. Contratto Titolare/Titolare: il fornitore assume il ruolo di titolare del trattamento ex art. 4 comma 7 del GDPR. Il fornitore ha autonomia nelle seguenti attività:
   - verifica conformità del trattamento
   - predisposizione misure tecniche e organizzative
   - responsabilità verso i soggetti interessati
   - notifica eventuali violazioni nel trattamento dallo stesso effettuato

In questo caso la Società dovrà adottare le nuove clausole contrattuali indipendenti del trattamento dei dati, definite in linea con le prescrizioni del GDPR.

b. Contratto Titolare/Responsabile: il fornitore tratta i dati in modo non autonomo ed in particolare:
   - assume il ruolo di responsabile del trattamento ex art. 4 c. 8 del GDPR;
   - rispetta le istruzioni scritte ricevute dal titolare;
   - garantisce competenza nell'adozione di misure tecniche e organizzative;
   - rispetta obblighi di collaborazione, informazione e notifica verso il Titolare;
   - nomina sub-responsabile autorizzato dal Titolare.

Al fine di rispettare i requirement del GDPR e le best practices in materia data protection, la Società ha definito:

- un censimento dei fornitori e delle terze parti che trattano i dati di titolarità della Società (c.d. registro fornitori e terze parti);
- nuove clausole contrattuali data protection da adottare nei contratti con i fornitori e le terze parti della Società.

Qualora i contratti con le terze parti prevedano delle clausole data protection differenti da quelle predisposte per la Società, è necessario coinvolgere la Funzione Legale e Compliance e la Funzione Acquisti per la revisione delle stesse al fine di garantire il rispetto delle misure necessarie per tutelare i dati personali trattati dalla Società.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella predisposizione e aggiornamento delle clausole contrattuali data protection con fornitori e terze parti.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 2: Modello Operativo						
Terze Parti	R	R	R	R/A	I	C

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.1.8 MISURE BY DESIGN

Al fine di assicurare un adeguato livello di sicurezza al trattamento di dati personali, devono essere adottate appropriate misure di sicurezza tecniche ed organizzative. In sede di identificazione delle misure da implementare è necessario adottare un approccio basato sul rischio, il quale dovrà tenere in considerazione la probabilità e la gravità dei rischi per i diritti e le libertà degli interessati, nonché lo stato dell'arte delle tecnologie e i relativi costi di attuazione.
La sicurezza informatica è un elemento fondamentale da tenere in considerazione in fase di gestione dei trattamenti sui sistemi informativi. All'interno di ciascun trattamento posto in essere dalla Società dovranno essere previste idonee misure di sicurezza tecniche[2], tenendo in considerazione finalità del trattamento, contesto e natura dei dati trattati.
Per il dettaglio relativo ai principi ed approccio privacy by design e by default fare riferimento al paragrafo 6.1 - Privacy by Design e by Default

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di definizione delle misure di sicurezza by design.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 2: Modello Operativo						
Misure by Design	I	C	C	C	R/A	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.2 MANUTENZIONE E AGGIORNAMENTO

A valle della decisione di implementare ulteriori misure organizzative/operative e/o tecniche al fine di mitigare il rischio data protection del trattamento, è necessario effettuare nuovamente la valutazione di gravità e probabilità per ciascun binomio minaccia-danno, al fine di valutare il rischio residuo connesso al trattamento.

Qualora non si renda necessario implementare ulteriori misure a tutela dei diritti e delle libertà degli interessati, il rischio rimarrà immutato.

Il Modello Operativo Data Protection definito nei paragrafi precedenti, affinché possa essere efficace deve essere oggetto di manutenzione periodica. Nello specifico l'intento è garantire e

[2] Sono stati presi a riferimento gli specifici articoli del GDPR in ambito security e le *best practice* di riferimento.

migliorare l'efficacia del Modello Operativo Data Protection a fronte di cambiamenti organizzativi, tecnologici e/o di business interni ed esterni/ normativi.

In particolare è necessario distingue due tipologie di aggiornamenti/ manutenzioni:

1. Manutenzione ordinaria: si tratta delle attività di aggiornamento che dovranno essere previste con cadenza periodica e in maniera continuativa;
2. Manutenzioni straordinaria: si tratta delle attività di aggiornamento che in occasione di modifiche rilevanti di natura tecnica o organizzativa, tali da rendere la documentazione inefficace, non aggiornata ed obsoleta in caso di verifiche ispettive.

3.2.1 MANUTENZIONE ORDINARIA

Il processo di manutenzione del Modello Operativo Data Protection deve essere basato su un programma annuale, definito in funzione di uno dei seguenti driver:

- Cambiamenti organizzativi;
- Cambiamenti tecnologici;
- Cambiamenti di business interni ed esterni;
- Cambiamenti normativi.

Nei paragrafi successivi sono descritte le analisi e i relativi documenti che necessitano di un aggiornamento periodico.

3.2.2 REVISIONE REGISTRO DEI TRATTAMENTI

La tenuta del registro dei trattamenti rappresenta un adempimento previsto come obbligatorio, in alcuni casi, dall'articolo 30 del GDPR. Esso è indice di una corretta gestione dei trattamenti.
In particolare:

- il registro dei trattamenti dovrà essere mantenuto ed aggiornato in forma scritta, anche in formato elettronico;
- il registro dei trattamenti dovrà essere esibito al Garante in caso di verifiche;
- si raccomanda di procedere alla revisione del registro dei trattamenti con cadenza almeno annuale.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella tenuta del registro dei trattamenti.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 3: Manutenzione e aggiornamento						
Registro dei trattamenti	I	R	R/A	C	I	-

Legenda:
R: Svolta da (Responsible)

A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.2.3 REVISIONE DPIA

Con riferimento alla DPIA si raccomanda in primo luogo l'aggiornamento del documento "Metodologia DPIA" approvato dalla Società, al fine di recepire eventuali cambiamenti organizzativi/tecnici, aggiornamenti/ adeguamenti delle normative di riferimento in materia di data protection.

Prima di procedere alla revisione della DPIA, è fondamentale procedere con la revisione della "Valutazione preliminare Privacy" ovvero l'analisi volta ad identificare il livello di rischiosità intrinseco del trattamento (rischio inerente).

La revisione della DPIA dovrà avvenire:

- ogni qualvolta si verifica una modifica del rischio presentato dall'attività di trattamento (Art. 35 (11) del GDPR), nella tipologia dei dati trattati, nelle modalità di trattamento, nelle soluzioni tecnologiche impiegate che possono aver modificato significativamente le analisi iniziali;
- in caso di modifica di uno dei componenti dell'attività di trattamento (dati, asset a supporto, fonti di rischio, potenziali impatti, minacce, ecc.);
- in caso di evoluzione del contesto del trattamento (scopo, funzionalità, ecc.). Ad esempio, i sistemi di elaborazione dati sono soggetti a rapide evoluzioni e potrebbero emergere nuove vulnerabilità;
- modifiche al contesto organizzativo o sociale dell'attività di trattamento (ad esempio se gli effetti di alcune decisioni automatizzate sono diventati più significativi, nuove categorie di persone fisiche diventano soggette a discriminazione o i dati vengono trasferiti a destinatari situati in un Paese che ha lasciato l'UE).

La DPIA, in virtù del principio di miglioramento continuo, dovrebbe essere riesaminata ogni anno, o prima (a seconda della natura del trattamento e del tasso di cambiamento delle attività di trattamento e delle circostanze generali) per tutti i trattamenti, anche qualora non si siano verificati cambiamenti significativi.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di aggiornamento della DPIA.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 3: Manutenzione e aggiornamento						
DPIA	I	R	R/A	C/I	C	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)

I: Informato (Informed)

3.2.4 REVISIONE INFORMATIVE E CONSENSI

Le informative e i consensi raccolti dovranno essere mantenuti aggiornati nel tempo, al fine di recepire eventuali cambiamenti in merito a:

- nuovi canali di raccolta;
- nuovi strumenti utilizzati;
- tipologie di interessato;
- natura del dato trattato;
- nuovi trattamenti di dati personali;
- eventuali revoche del consenso /autorizzazioni al trattamento.

Tali cambiamenti dovranno essere recepiti anche all'interno dei sistemi informativi, al fine di garantire all'interessato che il trattamento sia sempre corretto e trasparente.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di aggiornamento di informative e consensi.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 3: Manutenzione e aggiornamento						
Informative e Consensi	R	R	C	R/A	I	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.2.5 REVISIONE CLAUSOLE CONTRATTUALI CON FORNITORI E TERZE PARTI

Anche con riferimento alle clausole contrattuali di data protection si rende necessaria una revisione nei seguenti casi:

- previsione di un nuovo servizio che comporta un trattamento di dati personali;
- nuovo ruolo data protection del fornitore (es. per il nuovo servizio il fornitore assumerà il ruolo di titolare o responsabile del trattamento);
- nuove misure di sicurezza da adottare.

Il processo di aggiornamento è avviato dalla Funzione Acquisti, la quale formalizza i rapporti con il fornitore e delinea le esigenze della Società.

La Funzione Legale e Compliance interviene a supporto della Funzione Acquisti per definire, qualora il servizio implichi un trattamento di dati personali, il ruolo data protection del fornitore e procedere all'aggiornamento del contratto con il fornitore con le seguenti clausole:

- Titolare/Titolare nel caso in cui il fornitore assume il ruolo di titolare del trattamento ai sensi dell'art. 4 c. 7 del GDPR;
- Titolare/Responsabile nel caso in cui il fornitore tratta i dati in modo non autonomo, ma sulla base delle direttive ed istruzioni impartite dal titolare.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di aggiornamento delle clausole contrattuali data protection.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 3: Manutenzione e aggiornamento						
Terze Parti	-	I	C	R/A	-	R/C

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.2.6 REVISIONE MISURE DI SICUREZZA

Quanto alle misure di sicurezza è possibile che la Società decida di prevedere nuove misure di sicurezza a tutela dei dati personali. In particolare si rende necessaria una revisione delle misure di sicurezza nei seguenti casi:

- Nuove esigenze di business
- Nuovi trattamenti di dati personali
- Nuove tipologie di dati trattati

In questi casi specifici le Funzioni di Business, dovranno confrontarsi con la Funzione IT al fine di identificare le misure di sicurezza adeguate per garantire la sicurezza del trattamento.

Di seguito sono riassunti i ruoli e le responsabilità degli stakeholder coinvolti nella fase di aggiornamento delle misure di sicurezza.

Strutture organizzative / ***Attività***	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Fase 3: Manutenzione e aggiornamento						

Strutture organizzative / *Attività*	Incaricato	Data Manager	Referente Data Protection	Legale e Compliance	IT	Acquisti
Misure by Design	-	R	C	C	R/A	-

Legenda:
R: Svolta da (Responsible)
A: Responsabile (Accountable)
C: Consultato (Consulted)
I: Informato (Informed)

3.2.7 MANUTENZIONE STRAORDINARIA

La documentazione in ambito data protection (es. registro dei trattamenti, DPIA, informative e consensi, clausole contrattuali) oltre ad essere soggetta ad un processo di manutenzione ordinaria che ne prevede l'aggiornamento periodico, deve essere rivista in occasione di modifiche rilevanti di natura tecnica o organizzativa, tali da rendere la documentazione inefficace, non aggiornata ed obsoleta in caso di verifiche ispettive.

Di seguito sono descritti i fattori che possono attivare il processo di aggiornamento:

- **Variazioni risorse interne**: in caso di variazione delle risorse è necessario procedere all'aggiornamento delle nomine interne di cui al modello organizzativo data privacy, nonché alla sezione del registro dei trattamenti "A. DATI DI CONTATTO";
- **Variazioni fornitori**: ogni qualvolta si verifichino cambiamenti nelle condizioni contrattuali e/o siano sostituiti o acquisiti nuovi fornitori a supporto di processi che trattano dati personali è necessario prevedere delle clausole contrattuali data protection ad hoc. Al fine di comprendere quali clausole contrattuali utilizzare, è necessario definire il rapporto data protection tra la Società e fornitore (Titolare/ titolare o titolare responsabile). Inoltre il nuovo fornitore dovrà essere censito all'interno del registro dei fornitori della Società;
- **Variazioni nei rischi**: qualora emergano nuovi rischi nell'ambito delle attività di risk management sarà necessario valutare tali rischi rispetto alla data protection e conseguentemente aggiornare la documentazione correlata (es. valutazione preliminare del rischio, DPIA);
- **Variazioni organizzative**: si riportano a titolo esemplificativo:
  - La creazione di una nuova struttura organizzativa che impatta sulla protezione dei dati personali (accentramento/decentramento attività, ecc.).
  - L'esternalizzazione/internalizzazione della gestione, di tutto o parte, di servizi che trattano dati personali.
- **Variazioni Normativa Data Privacy**: eventuali nuove normative o modifiche alle normative in essere applicabili alla Società in tema data protection potrebbero avere un impatto sulla documentazione. Ciò comporta la necessità di aggiornamento della documentazione in ambito data protection;
- **Variazioni tecnologiche e applicative**: eventuali modifiche relative all'infrastruttura e agli applicativi utilizzati a supporto dei processi che trattano dati personali devono essere

segnalati dalla Funzione IT e/o dai Data Manager al fine di valutare le modifiche necessarie alla documentazione (registro dei trattamenti, mappatura delle misure tecniche).

4 ESERCIZIO DIRITTI DEGLI INTERESSATI

I diritti riconosciuti all'interessato nel GDPR possono considerarsi declinazioni particolari del più ampio diritto all'autodeterminazione informativa, inteso come il potere dell'individuo di governare il flusso delle proprie informazioni. Tali diritti appartengono a due macro-categorie:

1. **Diritti conoscitivi:**
   - Diritto all'informativa (artt.13-14);
   - Diritto di accesso (art.15);
   - Diritto alla comunicazione di una violazione dei dati (art. 34).

2. **Diritti di controllo:**
   - Diritto al consenso (artt. 6.1 lettera a; 9.2 lettera a);
   - Diritto di limitazione (art.18);
   - Diritto di revoca del consenso (art.7.3) e diritto di opposizione (art. 21);
   - Diritto alla portabilità (art. 20);
   - Diritti di rettifica e di integrazione (art.16);
   - Diritto di cancellazione/oblio (art.17).

La Società, per far fronte alle richieste che possono pervenire dagli interessati, sarà tenuta a:

- mettere a disposizione dei canali attraverso i quali gli interessati possano esercitare i propri diritti (es. indirizzi e-mail, Contact Center);
- definire e formalizzare un processo strutturato per la gestione operativa delle richieste degli interessati dal momento della loro ricezione fino al loro espletamento.

4.1 DIRITTI CONOSCITIVI

4.1.1 DIRITTO ALL'INFORMATIVA

Il titolare del trattamento, in caso di trattamento di dati personali ha l'obbligo di fornire un'informativa ai soggetti interessati, a prescindere che il trattamento sia fondato sul consenso o su altra condizione di liceità.

L'informativa è fornita gratuitamente all'interessato ed è resa per iscritto, ivi inclusi mezzi elettronici, oppure oralmente se ciò è richiesto dall'interessato di cui sia comprovata l'identità. Occorre osservare trasparenza, concisione, semplicità e chiarezza dell'informativa, e un linguaggio comprensibile a minori, ove essi siano gli interessati del trattamento.

Per maggiori dettagli su struttura e contenuti dell'informativa fare riferimento al paragrafo "3.1.5 Informative "

4.1.2 DIRITTO DI ACCESSO

Il diritto di accesso, tutelato espressamente all'art. 8.2 Carta UE e previsto dall'art. 15 del GDPR, costituisce una declinazione del medesimo diritto conoscitivo garantito con l'informativa, ma attuato ad iniziativa dell'interessato.

Quest'ultimo, ha il diritto di ottenere dalla Società conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, ottenere l'accesso ai dati 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 o 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 del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o 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 informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

La Società deve essere in grado di garantire che il diritto di accesso possa essere sempre esercitato e riconosciuto rispetto a qualsiasi trattamento di dati personali.

L'esercizio del diritto è a titolo gratuito così come il trasferimento da parte della Società di una copia dei dati all'interessato. (art. 15.3). Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

La Società, ha la facoltà di addebitare un ragionevole contributo spese o di rifiutare l'accesso, se dimostra che le richieste dell'interessato sono manifestamente infondate o eccessive.

La Società deve necessariamente adempiere alla richiesta di accesso dell'interessato senza ingiustificato ritardo, e comunque entro il termine di un mese previsto per il riscontro, prorogabile motivatamente, e con preavviso tempestivo, a due mesi.

Il rifiuto di ottemperare (es. per sussistente incertezza nell'identificazione dell'interessato) deve essere motivato e reso al più tardi entro un mese dall'istanza. Ove il trattamento consista in una notevole quantità di informazioni, all'interessato può essere richiesto di precisare le informazioni o le attività di trattamento a cui la richiesta si riferisce.

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

4.1.3 DIRITTO ALLA COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI

Nel caso in cui si verifichi una violazione dei dati che comporti un rischio elevato per i diritti e le libertà degli interessati, il titolare del trattamento ha l'obbligo di comunicare la violazione all'interessato. Per maggiori dettagli in merito alle modalità di comunicazione del titolare al soggetto interessato si rimanda alla "Procedura operativa Data Breach Management" adottata dalla Società.

4.2 DIRITTI DI CONTROLLO

4.2.1 DIRITTO AL CONSENSO

Il consenso, ai sensi dell'art. 6 del GDPR, costituisce una delle basi giuridiche che giustificano il trattamento dei dati personali e consiste in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso. In merito alla validità del consenso e le casistiche per le quali è necessario si rimanda al paragrafo 3.2.5 "Consensi".

4.2.2 DIRITTO DI LIMITAZIONE

Ai sensi dell'articolo 18 del GDPR, il diritto di limitazione, posto in capo all'interessato ed esercitabile verso il titolare del trattamento, consiste nella pretesa ad ottenere che il complessivo trattamento dei dati si riduca alla sola operazione di conservazione.

In particolare, l'interessato ha il diritto di ottenere dalla Società la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento 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;

d) l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Le lettere di cui al paragrafo a) e d) del presente Paragrafo rispondono ad esigenze di verifica dei dati, disponendo così una misura di favore per l'interessato. Diversamente, le altre due ipotesi delle lettere b) e c) rispondo all'esigenza di evitare l'attivazione di automatismi di cancellazione che potrebbero risultare pregiudizievoli per l'interessato.

L'esercizio del diritto è a titolo gratuito; tuttavia, la Società ha facoltà di addebitare un ragionevole contributo spese o di rifiutare l'istanza, se dimostra che le richieste dell'interessato sono manifestamente infondate o eccessive.

La Società dovrà inoltre informare dell'esercizio del diritto di limitazione a ciascuno dei soggetti a cui ha comunicato i dati (ad esempio fornitori e terze parti), salvo che ciò sia impossibile o implichi sforzo sproporzionato (art. 19). Il rifiuto di ottemperare (ad esempio per sussistente incertezza nell'identificazione dell'interessato) deve essere motivato e reso al più tardi entro un mese dall'istanza e indicare la possibilità di proporre un reclamo all'Autorità garante o un ricorso all'Autorità giudiziaria ordinaria.

Se il trattamento è limitato, tali dati personali potranno essere trattati dalla Società, 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.

La limitazione può essere successivamente revocata e, in tal caso, prima che la revoca abbia efficacia, la Società dovrà darne comunicazione al soggetto interessato.

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

4.2.3 DIRITTO DI REVOCA DEL CONSENSO E DIRITTO DI OPPOSIZIONE

Ai sensi dell'art. 7 comma 3 del GDPR, gli interessati che abbiano prestato il consenso allo svolgimento di determinate operazioni di trattamento hanno sempre la facoltà di revocarlo successivamente, per motivazioni legittime.

Il diritto è esercitato esclusivamente nei confronti del titolare, che può delegare i propri Data Manager, a svolgere funzioni di punto di contatto per l'interessato e a porre in essere le attività esecutive conseguenti all'esercizio del diritto.

Nel caso in cui si verifichi questa ipotesi, la Società dovrà prontamente interrompere le operazioni di trattamento svolte in virtù del consenso, salvo che non ricorrano condizioni di legittimo interesse che siano prevalenti rispetto agli interessi, ai diritti ed alle libertà fondamentali dell'interessato.

In tal senso è fondamentale l'adozione di uno strumento di data governance, necessario per la gestione centralizzata dei consensi.

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano, necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, compresa la profilazione.

Il diritto di opposizione al trattamento può essere esercitato dall'interessato solo nei casi tassativi previsti dall'art. 21 del GDPR:

1. **trattamento necessario per un interesse legittimo del titolare, inclusa la conseguente profilazione:** in questo caso l'opposizione può essere rifiutata dalla Società se dimostra l'esistenza di motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure in caso di accertamento, esercizio o difesa di un diritto in sede giudiziaria.
2. **trattamento per finalità di marketing diretto**: in questo caso l'interessato non è tenuto a motivare l'opposizione e la Società non potrà rifiutarla.
3. **trattamento per finalità di ricerca scientifica o storica o per finalità statistica:** in tale ipotesi l'interessato è tenuto a dichiarare i suoi specifici motivi di opposizione e la Società può rifiutare l'opposizione nel solo caso in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

L'opposizione ha efficacia dal momento della richiesta e fa cessare, in maniera definitiva e permanente il trattamento.

Con rifermento al tema della profilazione, ai sensi dell'articolo 22 del GDPR, l'interessato può opporsi a tale trattamento automatizzato di dati quando la profilazione produce effetti giuridici o incide in modo significativo sulla persona dell'utente.

La profilazione è ammessa quando:

1. il trattamento è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare;
2. il trattamento è autorizzato dal diritto dell'Unione o dello Stato Membro cui è soggetto il titolare del trattamento, che prevede altresì misure idonee a tutelare i diritti dei soggetti interessati;
3. vi è esplicito consenso al trattamento.

Nel primo e nel terzo caso, il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in particolare il titolare del trattamento deve

consentire il diritto dei singoli di esprimere il loro punto di vista, oltre che di ottenere ulteriori informazioni sulla decisione raggiunta sulla base di questa elaborazione automatica e il diritto di contestarla.

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

4.2.4 DIRITTO ALLA PORTABILITÀ

Il diritto alla portabilità, previsto dall'art. 20 del GDPR, consiste nella pretesa dell'interessato di ricevere dal titolare i dati personali in un formato strutturato, di uso comune e leggibile da un dispositivo automatico e di ottenere, ove tecnicamente fattibile, la trasmissione diretta e senza impedimenti ad altro titolare indicato dall'interessato.

In primo luogo, comprende il diritto dell'interessato di ricevere un sottoinsieme dei dati personali che lo riguardano trattati da un titolare, e di conservarli in vista di un utilizzo ulteriore per scopi personali.

In secondo luogo, attribuisce agli interessati il diritto di trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento senza impedimenti. Questa componente del diritto configura per gli interessati la possibilità non soltanto di ottenere e riutilizzare i dati forniti a un titolare del trattamento, bensì anche di trasmettere questi dati a un diverso fornitore di servizi (appartenente allo stesso o a un diverso settore di attività).

Il nuovo diritto alla portabilità intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro.

In quest'ottica la Società dovrà:

- informare sempre dell'esistenza del diritto alla portabilità prima di procedere alla chiusura di un account;
- spiegare con chiarezza la differenza fra le categorie di dati che un interessato può ricevere attraverso l'esercizio del diritto alla portabilità anziché del diritto di accesso;
- i titolari "riceventi" dovrebbero fornire agli interessati un'informativa completa sulla natura dei dati personali pertinenti ai fini della prestazione del rispettivo servizio.

Ai sensi dell'art. 20.1 del GDPR, il diritto di portabilità si applica unicamente ai trattamenti automatizzati di dati comuni e sensibili fondati sul consenso o su un contratto.

La Società nel caso in cui darà esecuzione alle richieste di portabilità nei termini di cui all'art. 20 del GDPR, non è responsabile del trattamento effettuato dal singolo interessato o da un'altra società che riceva i dati in questione. La Società pertanto, agendo per conto dell'interessato, non è responsabile dell'osservanza delle norme in materia di protezione dei dati da parte del titolare ricevente, non essendo quest'ultimo da lui selezionato.

La Società inoltre, potrà dare esecuzione al diritto di portabilità solo nel caso in cui la richiesta di portabilità avvenga da parte dell'interessato.

Infine, la Società dovrà fornire all'interessato le informazioni relative all'azione intrapresa senza ingiustificato ritardo, e comunque entro il termine di un mese previsto per il riscontro, prorogabile motivatamente, e con preavviso tempestivo, a due mesi.

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

4.2.5 DIRITTO DI RETTIFICA E DI INTEGRAZIONE

Il diritto di rettifica, ai sensi dell'art. 16 del GDPR, attribuisce all'interessato il potere di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Per rettifica si intende sia correzione di inesattezze sia integrazione di informazioni non complete.

La Società dovrà pertanto adempiere alla richiesta senza ingiustificato ritardo e comunque entro il termine di un mese previsto per il riscontro, prorogabile motivatamente, e con preavviso tempestivo a due mesi.

La Società, a fronte di richieste di rettifica ed integrazione, deve rendere nota la rettifica/integrazione a ciascuno dei soggetti a cui ha comunicato i dati (es. fornitori e terze parti), salvo ove ciò sia impossibile o implichi sforzo sproporzionato (art. 19). Il rifiuto di ottemperare (ad es. per sussistente incertezza nell'identificazione dell'interessato) deve essere motivato e reso al più tardi entro un mese dall'istanza.

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

4.2.6 DIRITTO DI CANCELLAZIONE E OBLIO

L'interessato ha il diritto di ottenere dal Titolare del Trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare i dati personali, nei casi tassativi previsti dall'art. 17 comma 1 del GDPR.

Per maggiori dettagli in merito ai casi in cui è esercitabile il diritto di cancellazione e oblio e alle tempistiche/modalità di cancellazione si rimanda al capitolo "6.3 Data Retention".

Per maggiori dettagli in merito all'esercizio di tale diritto da parte dell'interessato e alla gestione da parte della Società di tale richiesta, si rimanda alla "Procedura operativa sull'esercizio dei diritti degli interessati" adottata dalla Società.

5 DATA BREACH

Il GDPR, artt. 33 e 34 prevede che in caso di violazione dei dati personali (data breach) il titolare del trattamento notifica la violazione all'autorità di controllo.
In particolare, se l'incidente di sicurezza (di seguito "privacy incident") comporta in maniera irreversibile la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali dei soggetti interessati al trattamento della Società, lo stesso ricade nell'ambito del data breach.

A titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazioni di dati personali (o "privacy incident"):

- **distruzione di dati informatici o documenti cartacei** (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);
- **perdita di dati, conseguente a smarrimento/furto di supporti informatici** (es. laptop, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- **accesso non autorizzato o intrusione a sistemi informatici,** lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi;
- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o intervento umano;
- **rivelazione di dati e documenti a soggetti terzi non legittimati,** anche non identificati, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo a soggetti diversi dall'effettivo destinatario o errata gestione di supporti informatici.

La Società, al fine di gestire correttamente eventuali casi di violazione di dati personali, ha definito un processo di data breach management, necessario per fornire agli utenti le indicazioni operative e le informazioni necessarie per assicurare il proprio ruolo all'interno del processo di data breach management. In particolare, la Società ha definito un processo per la gestione delle violazioni di dati personali, il quale si articola in cinque fasi di seguito riportate:

- **Fase 1 - Identificazione:** l'obiettivo di questa fase è quello di identificare, tramite una valutazione preliminare, se le segnalazioni ricevute possano essere definite come privacy incident;
- **Fase 2 - Valutazione:** l'obiettivo di questa fase è di effettuare la valutazione della rilevanza del privacy incident, tramite la stima del potenziale rischio associato ai diritti e libertà delle persone fisiche. A tal fine la Società ha definito una "Metodologia per la valutazione della gravità delle violazioni dei dati personali", la quale è fondamentale per stabilire se notificare o meno il data breach all'Autorità Garante ed eventualmente agli interessati coinvolti;
- **Fase 3 - Risposta**: l'obiettivo di questa fase è la formalizzazione del report e la notifica all'autorità Garante del data breach tramite l'apposito modulo, e nel caso fosse necessario, la comunicazione all'interessato;
- **Fase 4 - Risoluzione:** l'obiettivo di questa fase è la formalizzazione del piano di azione correttiva con l'obiettivo di mitigare il rischio individuato e di predisporre delle tempestive azioni in modo da contenere e gestire al meglio il privacy incident individuato;
- **Fase 5 - Post incident review:** l'obiettivo di questa è svolgere un esame ex post della gestione del privacy incident al fine di predisporre un report di chiusura dell'incident da inviare ai Data Manager coinvolti con le principali cause dell'evento, le azioni implementate per superare le criticità emerse ed eventuali opportunità di miglioramento dei processi aziendali.

La Società ha inoltre definito un "Registro dei data breach", necessario per tenere traccia delle violazioni di dati personali avvenute all'interno del contesto aziendale.

Ai sensi dell'articolo 55 del GDPR, la notifica deve avvenire senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne siano venuti a conoscenza, a meno che sia

improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Ai sensi dell'art. 33 comma 1, la Società non è tenuto ad effettuare la notifica all'Autorità se è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ma deve ugualmente tenerne traccia documentale all'interno del registro dei data breach.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo.

Inoltre, nel caso in cui la violazione dei dati personali possa generare un rischio elevato per i diritti e le libertà delle persone fisiche, la Società (in qualità di titolare del trattamento) dovrà darne comunicazione all'interessato senza ingiustificato ritardo.

Nel caso in cui la Società abbia affidato dei servizi ad un fornitore, quest'ultimo dovrà segnalare tempestivamente alla Società eventuali casi di data breach secondo quanto previsto dagli artt. 33 e 34[3] del GDPR.

Per maggiori dettagli sul processo di Data Breach Management e per la "Metodologia per la valutazione della gravità delle violazioni dei dati personali", si rimanda al documento "Procedura Operativa sul Data Breach Management" adottata dalla Società.

6 DOMINI DI GESTIONE DATA PROTECTION

Il presente capitolo ha l'obiettivo di indirizzare la Società in merito alle principali prescrizioni e adempimenti normativi in materia di:

- Privacy by design e by default;
- Autorizzazione, autenticazione e gestione degli accessi;
- Anonimizzazione e pseudonimizzazione;
- Data retention;
- Trasferimenti di dati extra UE.

Al fine di assicurare un adeguato livello di sicurezza al trattamento di dati personali, devono essere adottate appropriate misure di sicurezza tecniche ed organizzative. In sede di identificazione delle misure da implementare è necessario adottare un approccio basato sul rischio, il quale dovrà tenere in considerazione la probabilità e la gravità dei rischi per i diritti e le libertà degli interessati, nonché lo stato dell'arte delle tecnologie e i relativi costi di attuazione.

6.1 PRIVACY BY DESIGN E BY DEFAULT

Con riferimento al principio privacy by design e by default di cui all'art. 25 del GDPR, si intende per:

- **Privacy by design**: la necessità di tutelare il dato sin dalla progettazione dei sistemi informatici che ne prevedono l'utilizzo. In particolare il titolare del trattamento dovrà essere in grado di adottare ed attuare misure tecniche e organizzative che tutelino i principi di protezione dei dati sin dal momento della progettazione oltre che in fase di esecuzione del trattamento. In base al principio della privacy by design l'utente deve essere considerato al centro del sistema data protection, pertanto ogni qualvolta si avvia un progetto occorre prendere in considerazione, prima di tutto, il ruolo dell'utente, tenendo fin da subito in considerazione i diritti e le libertà degli interessati;

[3] WP250 Guidelines on Personal data breach notification under Regulation 2016/679

- **Privacy by default**: le impostazioni di tutela della vita privata relative ai servizi e prodotti devono rispettare i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità. Il titolare, in attuazione di tale principio, deve prevedere la protezione rafforzata di determinate informazioni all'interno dei sistemi informatici e prevedere dei default settings, ovvero delle impostazioni automatiche a maggior tutela dei dati dell'interessato.

La privacy by design e by default prevede un approccio "privacy embedded" di integrazione *ex ante* delle logiche data protection, che obblighi il titolare, nella fase iniziale di determinazione delle finalità e delle modalità del trattamento, a valutare i rischi alla luce dell'ambito specifico di applicazione delle tecnologie disponibili, mettendo in atto le misure tecnico-organizzative che garantiscano un'adeguata tutela agli interessati.
In particolare tali misure dovranno perseguire i seguenti obiettivi:

- ridurre il più possibile il trattamento di dati personali;
- pseudonimizzare i dati il più presto possibile;
- garantire una maggior sicurezza del trattamento (art. 32 GDPR).

Il principio di privacy by design e by default deve essere tenuto in considerazione nei seguenti casi:

- In fase di progettazione dei sistemi informatici per l'archiviazione o l'accesso ai dati personali dei clienti;
- In caso di iniziative che richiedono la condivisione o il trattamento di dati personali;
- In fase progettuale in cui si prospetta l'implementazione di nuove tecnologie invasive (ad esempio riconoscimento biometrico, sistemi di videosorveglianza, ecc.);
- Nelle prime fasi di elaborazione dei dati per nuovi scopi (es. nuove iniziative di marketing/ nuovi prodotti assicurativi).

La privacy by design e by default offre benefici significativi in particolare:

- Identificazione immediata delle potenziali criticità e rischio di sanzioni già nella fase iniziale di progettazione di un nuovo progetto, prodotto, servizio. Questo implica una riduzione dei costi per le sanzioni;
- Aumento della consapevolezza e sensibilità in materia di protezione dei dati all'interno dell'azienda come conseguenza diretta, con conseguente risparmio di costi per corsi di formazione o consulenza esterna;
- Maggiori conformità a prescrizioni normative e minore probabilità di violazione di leggi e regolamenti durante lo sviluppo dei propri progetti commerciali;
- Minore intrusività dei progetti in materia di dati personali e minore impatto negativo sugli individui. Questo implica una maggiore fiducia dei clienti.

6.1.1 I Principi Fondamentali

Nell'ambito della privacy by design la Società adotta i seguenti principi fondamentali, i quali dovranno essere tenuti in considerazione in fase di sviluppo di ogni nuovo progetto/ trattamento/ processo.

Principio	Descrizione
1. Preventivo	L'approccio di privacy by design è caratterizzato da misure proattive piuttosto che reattive. Essa è diretta ad anticipare e previene gli eventi invasivi della privacy prima che accadano.

non correttivo	Non attende che i rischi per la privacy si materializzino, né offre rimedi per la risoluzione delle infrazioni della privacy una volta che si sono verificati, in quanto è diretta ad impedire che si verifichino.
2. Privacy come impostazione predefinita	La privacy by design è diretta a garantire il massimo grado di privacy prevedendo che i dati personali siano automaticamente protetti in qualsiasi sistema IT o di business. Nessuna azione è richiesta da parte dei singoli per proteggere la loro privacy, in quanto è integrata nei sistemi per impostazione predefinita. L'impostazione predefinita è basata su: • Finalità del trattamento: la finalità per la quale i dati personali sono raccolti, trattati, conservati e divulgati dalla società deve essere specificata e comunicata all'interessato, al momento o prima della raccolta dei dati personali. Le finalità del trattamento devono essere chiare, limitate e pertinenti alle circostanze. • Limitazione della raccolta: la raccolta di dati personali deve essere chiara, lecita e limitata a ciò che è necessario per la finalità del trattamento. • Data minimization: dovrà essere raccolta la minore quantità possibile di dati personali necessari per il corretto funzionamento del sistema. • Limitazione del trattamento: l'utilizzo, la conservazione e la divulgazione di dati personali devono essere limitati alle finalità per i quali l'individuo ha acconsentito al trattamento. In quest'ottica è fondamentale che tutti i set di dati personali presenti nei sistemi dispongano di una policy di data retention, la quale risulta essere fondamentale per identificare quali dati cancellare, una volta cessato il periodo di conservazione previsto.
3. Privacy incorporata nel design	La privacy by design è incorporata nel design e nell'architettura dei sistemi IT e di business. Non è attuata successivamente ad un evento. Il risultato è che la privacy diventa una componente essenziale delle funzionalità principali. La privacy è parte integrante del sistema, senza diminuirne la funzionalità.
4. Funzionalità completa, somma positiva non somma zero	La privacy by design mira a creare un approccio a somma-positiva, dove non è necessario sacrificare tutti gli obiettivi a discapito di uno solo, ma è possibile tutelarli entrambi. Nell'ottica privacy by design è possibile tutelare sia la sicurezza che la privacy, senza rinunciare ad uno dei due obiettivi.
5. Sicurezza end-to-end, protezione completa del ciclo di vita	La privacy by design che è stata incorporata in un sistema sin dal primo momento, si estende in modo sicuro durante l'intero ciclo di vita dei dati coinvolti: è necessario che la Società preveda delle robuste misure di sicurezza - essenziali per la privacy - dall'inizio alla fine del ciclo di vita del dato. Ciò garantisce che tutti i dati vengano conservati e distrutti - in modo sicuro e tempestivamente - alla fine del processo. Pertanto, la privacy by design garantisce una gestione delle informazioni sicura end-to-end.
6. Visibilità e trasparenza – Keep it Open	La privacy by design cerca di assicurare a tutti gli stakeholder che qualunque sia la pratica aziendale o la tecnologia coinvolta, essa opererà secondo le promesse e gli obiettivi dichiarati, anche assoggettandosi a verifiche indipendenti. Le sue componenti e le sue operazioni rimangono visibili e trasparenti, sia per gli utenti che per i fornitori. La trasparenza è essenziale per mantenere la fiducia del cliente e degli stakeholder coinvolti. Nello specifico, è necessario si focalizza sui seguenti concetti: • Responsabilità/accountability: la responsabilità di tutte le politiche e procedure relative alla protezione dei dati deve essere documentata e comunicata. • Trasparenza: il titolare del trattamento dovrà fornire informazioni sulle politiche e le pratiche relative alla gestione dei dati personali dei clienti, utilizzando un linguaggio chiaro.
7. Rispetto per la privacy degli utenti - Mantenerlo incentrato sull'utente	La privacy by design richiede ai progettisti e agli operatori di garantire gli interessi dei singoli, offrendo robuste misure di privacy per impostazione predefinita. Prevedendo degli avvisi appropriati e potenziando le opzioni user-friendly, pertanto garantendo l'impostazione user-centric. Tale approccio pone le sue basi sui seguenti concetti: • Consenso: è richiesto il consenso libero, specifico ed esplicito del cliente per la raccolta, l'uso o la divulgazione dei dati, salvo ove diversamente stabilito dal GDPR. Il cliente deve poter revocare il proprio consenso e la Società deve essere in grado di garantire che tale scelta del cliente sia recepita all'interno dei sistemi, attività e

	processi coinvolti. • Accesso: gli interessati hanno il diritto di accedere ai propri dati personali trattati dalla Società, nonché devono essere informati in merito al loro utilizzo ed eventuale divulgazioni/ comunicazione a soggetti terzi. • Gestione dei diritti degli interessati: la Società dovrà essere in grado di assicurare che esistano delle funzionalità in grado di rispondere alle richieste del cliente e, se necessario, funzionalità tecniche per la gestione delle richieste di portabilità dei dati. Ove possibile, è meglio limitare i flussi transfrontalieri di dati personali. Per quanto riguarda le modalità di gestione dei diritti degli interessati, fare riferimento alla procedura sulla gestione dei diritti degli interessati.

Nell'ambito della privacy by default, la Società adotta i seguenti principi fondanti, al fine di garantire che vengano trattati per impostazione predefinita solo i dati personali strettamente necessari, per le finalità previste e per il periodo strettamente necessario. Tali principi si ispirano allo standard ISO/IEC 29100:2011[4] .

Principio	Descrizione	Rischi
1. Consenso e scelta	Il principio del consenso prevede di presentare all'interessato la scelta se acconsentire o meno al trattamento dei propri dati personali (Consenso Informato). Aderire al principio della scelta significa fornire all'interessato – in maniera chiara, facilmente comprensibile, accessibile e conveniente - i meccanismi per esercitare la scelta e di fornire il consenso in relazione al trattamento dei suoi dati personali al momento della raccolta, al primo utilizzo o non appena possibile.	La mancata prestazione del consenso dell'interessato può: • minare il rapporto fiduciario titolare-interessato e possibili reazioni negative dell'interessato sia in forma diretta, sia tramite azioni che possono danneggiare la reputazione del titolare. • diminuire l'efficacia di alcune attività operative aziendali, come ad esempio le operazioni di marketing, in quanto i messaggi promozionali, relativi ai prodotti, vengono inviati a soggetti che non sono specificamente interessati. • possibili responsabilità legali con relative sanzioni, soprattutto laddove l'obbligo di raccogliere consenso è richiesto da specifiche disposizioni di legge o codici di autoregolamentazione. Il fatto di non aver ottenuto un consenso implicito potrebbe costituire una motivazione, per gli interessati, a negare qualsiasi altro tipo di consenso per futuri utilizzi dei dati personali.
2. Scopo legittimo e specifico	Il principio di legittimità e specificità dello scopo assicura che quest'ultimo sia conforme alla legge applicabile e si basi su una base giuridica ammissibile.	I rischi potenziali sono numerosi e legati al fatto che vengano raccolti dati personali eccedenti rispetto a quelli strettamente necessari per soddisfare le finalità del trattamento con il rischio di esporre la Società ad un maggiore livello di responsabilità, a maggiori rischi afferenti alla sicurezza e ad una possibile violazione del principio della data protection by default nonchè costi aggiunti di amministrazione dei dati Se le finalità della raccolta non vengono chiaramente comunicate agli interessati, può crearsi una situazione di sfiducia, che può portare a una perdita della fiducia del cliente.
3. Limitazione della raccolta	Il principio della limitazione della raccolta prevede la limitazione della	I rischi connessi a un'eccessiva raccolta di dati discendono dal fatto che, quanto maggiore è la quantità di dati raccolti, tanto maggiore potrebbero essere i problemi che potrebbero nascere, ove si creino delle anomalie in fase di trattamento e conservazione. Il fatto

[4] https://www.iso.org/standard/45123.html

	raccolta dei dati personali a ciò che è strettamente necessario per gli scopi specificati.	di raccogliere un numero eccessivo di dati personali espone quindi la Società ad un costo maggiore di gestione ed a maggiori responsabilità operative. Maggiore è la quantità di dati personali raccolta, tanto maggiore è la probabilità che possano verificarsi degli errori oppure che non venga rispettato il principio di accuratezza del dato. La raccolta di dati non trasparente o eccessiva può: • esporre la Società a sanzioni conseguenti all' attuazione di pratiche operative ingannevoli. • creare danni all'immagine dell'azienda con una significativa reazione negativa da parte degli interessati e dai clienti in genere, ove queste informazioni vengano pubblicizzate • possibilità di riduzione del giro d'affari Le considerazioni sopra illustrate si applicano non soltanto alle informazioni che vengono raccolte con metodi tradizionali, vale a dire su supporti cartacei, ma ancora di più si applicano alle informazioni raccolte mediante strumenti elettronici, come ad esempio i cookies presenti su molte pagine web. L'omessa informazione circa tale attività può anch'essa creare reazioni fortemente negative nei navigatori del sito web.
4.Minimizzazione dei dati	Il principio della minimizzazione dei dati prevede la progettazione, l'implementazione e l'elaborazione dei dati, attraverso procedure o sistemi ICT, in modo da ridurre al minimo i dati personali che vengono elaborati e il numero di parti interessate della privacy.	Il trattamento e la comunicazione di dati personali eccedenti rispetto alle finalità definite in fase di raccolta possono: • compromettere la fiducia degli interessati • portare a denunce per pratiche commerciali ingannevoli • rischio che i dati vengano conservati per un per un periodo eccedente rispetto a quello necessario per la finalità raccolta, sostenendo quindi costi aggiuntivi di archiviazione. • Al contrario, in caso di mancata definizione della durata dei dati personali raccolti è possibile che vengano distrutti in maniera prematura dati personali, compromettendo la possibilità degli interessati di accedere a questi dati e limitando la disponibilità di dati, che potrebbero essere necessari per gestire in modo efficiente ed efficace le finalità dichiarate. Le procedure di distruzione devono essere garantistiche e conformi alle vigenti normative europee, che costituiscono stato dell'arte per la procedura di distruzione.
5. Precisione e qualità	Il principio di accuratezza e qualità assicura che i dati personali elaborati siano accurati, completi, aggiornati (a meno che non vi sia una base legittima per mantenere dati obsoleti), adeguati e pertinenti alle finalità del trattamento.	L'utilizzo di dati non accurati, al fine di prendere decisioni afferenti ai clienti dell'azienda, può portare a perdite di profitti e perdita di quote di mercato. Dati personali non accurati possono danneggiare il cliente e compromettere la relazione con lo stesso. La Società deve pertanto identificare i requisiti di aggiornamento dei dati, al fine di evitare aggiornamenti non necessari disperdendo risorse e evitando di infastidire i clienti coinvolti.
6. Apertura, trasparenza e	Tale principio prevede di fornire informazioni chiare e facilmente	Una mancanza di trasparenza nel comportamento della Società potrebbe avere i seguenti impatti:

preavviso	accessibili sulle politiche stabilite dal titolare del trattamento e sulle procedure e pratiche relative al trattamento dei dati personali.	• impedire agli interessati di comprendere a fondo come la Società tratta e protegge i dati personali affidati dall'interessato stesso • diminuire la possibilità di ottenere un consenso al trattamento stesso. • Riduzione del livello di fiducia del cliente e • Compromissione del rapporto fra la Società e il cliente stesso. Parimenti, la mancanza di trasparenza può far sì che il cliente possano rendersi conto del fatto che alcuni dati possono essere comunicati a terzi, creando potenziali disguidi e malintesi, che influenzano negativamente l'immagine aziendale.
8. Partecipazione individuale e accesso	Il principio della partecipazione e dell'accesso individuale prevede di fornire agli interessati la possibilità di accedere e di rivedere i propri dati personali, a condizione che la loro identità sia autenticata con un livello adeguato di garanzia e tale accesso non sia vietato dalla legge applicabile.	La mancata elaborazione ed attuazione di una procedura per la gestione dei diritti di accesso dell'interessato può portare ad un trattamento dati personali non siano corretti o aggiornati. Il mancato rispetto, entro limiti temporali ben definiti, di una richiesta di accesso a dati personali può portare all'applicazione di significative sanzioni.
9. Responsabilizzazione	Il principio dell'*accountability* prevede di documentare e comunicare in modo appropriato tutte le politiche, le procedure e le pratiche adottate in ambito data protection. Prevede altresì l'assegnazione ad un individuo specifico all'interno dell'organizzazione del compito di attuare le politiche, le procedure e le best practice in materia di protezione dei dati.	In materia di responsabilizzazione, il rischio associato potrebbe comportare: • Violazione del rapporto fiduciario con i clienti • Rivelazione non autorizzata di dati personali, trattamenti non consentiti o illeciti • Danno all'immagine e alle relazioni di affari della Società • Difficoltà di gestione delle lamentele della clientela provocando insoddisfazione con potenziale perdita di affari
10. Sicurezza delle informazioni	Il principio di sicurezza delle informazioni prevede di proteggere i dati personali sotto la propria responsabilità con dei controlli appropriati a livello operativo, funzionale e strategico. L'obiettivo è quello di garantire l'integrità, la riservatezza e la disponibilità dei dati personali e proteggerli dai rischi, quali l'accesso non autorizzato, la distruzione, l'utilizzo non consentito, la modifica, la divulgazione o la perdita in tutto il ciclo di vita dell'informazione	Il mancato utilizzo di appropriati meccanismi di controllo dell'accesso comporta il rischio che soggetti terzi non autorizzati possono accedere ai dati personali e utilizzarli per finalità non previamente autorizzate. Tali azioni possono creare un danno significativo all'interessato ed essere fonte di responsabilità potenziale per la Società.
11. Conformità alla normativa	Il principio della conformità alla normativa prevede di verificare e dimostrare che il trattamento rispetti la protezione dei dati e la tutela della privacy, attraverso requisiti specifici e mediante verifiche periodiche - anche attraverso il ricorso a revisori	Se non si ha a disposizione un efficiente sistema di verifica della congruità con disposizioni regolamentari, potrebbe essere difficile determinare: • il rispetto dei dettati in materia di raccolta, trattamento, comunicazione e conservazione dei dati personali • problemi di natura legale, che potrebbero portare all'applicazione di significative sanzioni

	interni o esterni.	• riflessi negativi sulla qualità e continuità del rapporto di affari
12. Gestione dei data breach	L'obiettivo dell'articolo 33 del GDPR è quello di porre tempestivo riparo alle conseguenze, potenzialmente gravi, di una violazione di dati personali (data breach). Occorre pertanto rilevare che le conseguenze della violazione di dati possono essere estremamente diversificate, in funzione del fatto che la violazione comporti la perdita di un dato, piuttosto che la sottrazione ed il possibile utilizzo abusivo da parte di chi ha sottratto il dato.	In caso di violazione del trattamento dati personali, essa deve essere notificata nel termine massimo di 72 ore da quando la violazione dei dati si è verificata, oppure dal momento in cui il titolare o il responsabile del trattamento si è accorto di tale violazione. Pertanto è fondamentale stabilire modalità e tempi per la comunicazione della violazione ai soggetti interessati (fare riferimento alla Procedura gestione dei data breach)
13. Trasferimento dati all'estero	I dati personali possono essere trasferiti anche al di fuori dell'Unione Europea, in paesi terzi, a condizione che tali paesi siano stati sottoposti a una valutazione di idoneità delle disposizioni di legge, ivi esistenti ed afferenti alla protezione dei dati personali e che siano implementate garanzie adeguate.	I rischi potenziali sono principalmente: • rischi legati al fatto che il paese terzo in questione non garantisce una sufficiente protezione dei dati personali, • rischi legati al fatto che l'introduzione di eventuali regole e leggi cogenti, che permettono di trasferire dati personali in paesi terzi, non siano rispettate. Il verificarsi di entrambi i rischi può portare a conseguenze estremamente gravi, in termini di perdita di immagine e di applicazione di sanzioni, che possono raggiungere importi estremamente elevati.

6.1.2 COSA SIGNIFICA ADOTTARE UN APPROCCIO PRIVACY BY DESIGN E BY DEFAULT

La privacy by design e by default rappresenta un approccio metodologico-strategico proattivo che posiziona l'interessato al centro del sistema stesso (approccio user centric), così da anticipare e prevenire l'insorgenza di potenziali lesioni dei suoi diritti.
Ciascun Titolare del trattamento dei dati personali, anche in virtù del principio di accountability, dovrà pertanto adottare:

- un approccio basato sul rischio;
- una visione orientata alla protezione dei dati personali.

Tale approccio deve essere adottato dalla Società in fase di progettazione e implementazione di nuovi progetti/ prodotti/trattamenti.
L'approccio si declina in 4 fasi:

Figura 3: Approccio alla Privacy by design e by default

1. **Idea:** si tratta della fase iniziale del progetto, dove si definiscono i *business case*. È quindi la vera e propria fase di "design dell'idea". Se l'idea di partenza è basata su un trattamento che non può essere considerato lecito rispetto ai principi del GDPR, sarà destinata al fallimento. L'idea deve necessariamente essere accompagnata da una fase di analisi, durante la quale devono essere individuate ed analizzate tutte le possibili criticità ed i rischi connessi alla protezione dei dati personali, in maniera tale da essere affrontati già in fase di progettazione e implementazione. In questa fase si rende pertanto necessario per la Società condurre una DPIA ogni volta un nuovo processo aziendale/ trattamento (nel caso in cui si richieda l'elaborazione dei dati), rischia di comportare un rischio elevato per i diritti e le libertà degli interessati. Qualora vi siano criticità in ambito data protection, sarà opportuno bloccare

l'idea già in questa fase, piuttosto che successivamente, quando sono già state investite le risorse necessarie per le fasi successive;

2. **Requisiti:** in questa fase devono essere definiti i dettagli e requisiti normativi, pertanto è opportuno coinvolgere la Funzione Legale e Compliance, nonché la Funzione IT e la Funzione Business. Durante questa fase tali soggetti devono comprendere quali requisiti e limitazioni esistono, quali accorgimenti possono essere presi, e come deve essere disegnato il prodotto per poter garantire un trattamento dei dati conforme al GDPR e ai principi in esso contenuti. In questa fase dovranno essere definite le misure by design (fare riferimento all'Allegato Tabella di dettaglio Misure By Design).
3. **Disegno e sviluppo:** in questa fase viene definita l'architettura del sistema, le componenti, i moduli, le interfacce o i processi specifici di un progetto per soddisfare i requisiti del GDPR e le best practices in materia di sicurezza informatica.
   Nel corso della fase di progettazione è necessario quindi garantire un adeguato livello di sicurezza applicativa e infrastrutturale attraverso l'analisi e la modellazione delle minacce inerenti gli applicativi coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema.
   L' approccio privacy by design implica pertanto la necessità di investimenti nello sviluppo dei servizi ICT, lato security, che permettano di costituire adeguati presidi.
   Nella fase di disegno e sviluppo rientra la scrittura e la sicurezza del codice, la quale è fondamentale per comprendere:
   a. come viaggeranno i dati;
   b. chi potrà consultarli e trattarli durante il tragitto;
   c. i soggetti terzi coinvolti.

   In fase di sviluppo dell'applicazione sarà quindi necessario adottare delle misure in grado di:

   - ridurre al minimo l'impatto sulle risorse di sistema;
   - evitare che i dati di accesso siano inseriti all'interno dei sorgenti;
   - evitare l'utilizzo di privilegi amministrativi;
   - assicurare l'assenza di codice malevolo;
   - garantire che eventuali errori ed eccezioni non danneggino l'integrità delle informazioni gestite dall'applicazione;
   - garantire che i parametri di input inseriti dall'utente siano conformi a quanto atteso;
   - assicurare che l'output prodotto contenga le sole informazioni rilevanti per l'utente;
   - assicurare che il codice rispetti i criteri di formattazione, sintassi, algoritmi e gestione delle stringhe e delle variabili stabiliti dall'azienda;
   - assicurare la rilevazione di eventi anomali significativi per la sicurezza dell'organizzazione.

   In questa fase di disegno e sviluppo è di fondamentale importanza il supporto della Funzione IT, la quale deve essere in grado di offrire i giusti suggerimenti prima che il codice venga scritto. Viene anche valutato il c.d. "look and feel" del prodotto o servizio, come gli utenti si rapportano e lo utilizzano: quella che generalmente viene definita "user experience," "user interface," o semplicemente UX o UI. In questa fase è fondamentale il confronto tra le Funzioni di Business da cui è nata l'idea, la Funzione IT e la Funzione Legale e Compliance.
4. **Test e adozione:** si tratta della fase di messa in produzione del servizio o del prodotto per verificarne le performance. In particolare deve essere garantito che il sistema soddisfi i requisiti in materia data protection e sicurezza.

In merito agli ambienti operativi di sviluppo e test delle applicazioni, sarà pertanto necessario garantire:

- la separazione degli ambienti di sviluppo, test e produzione, fisicamente e/o logicamente;
- il passaggio in produzione solo successivamente al buon esito di test relativi alla rispondenza ai requisiti dati, all'usabilità, alla sicurezza e la compatibilità con l'infrastruttura;
- i profili utente dei sistemi di produzione siano diversi da quelli definiti e utilizzati negli ambienti di test e sviluppo;
- i dati personali e critici presenti in ambiente di sviluppo e test non siano dati reali copiati dagli ambienti di esercizio;
- i sorgenti dell'applicazione non siano in chiaro in ambiente di produzione.

La Società dovrà infine prevedere un piano di azione per rispondere alle eventuali criticità emerse in materia data protection o sicurezza informatica, al fine di garantire che qualsiasi evoluzione del sistema o modifica dei processi sia monitorata e controllata per comprendere se ha un impatto sul livello di protezione dei dati.

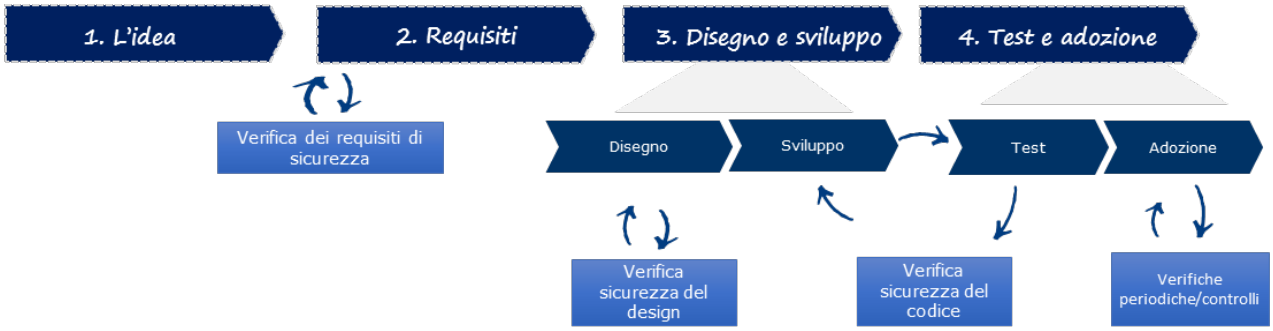


Figura 4: Step Approccio Privacy by Design e by Default

6.2 AUTENTICAZIONE, AUTORIZZAZIONE E GESTIONE DEGLI ACCESSI

La sicurezza del patrimonio informativo aziendale e dei relativi dati personali trattati si fonda sull'insieme di principi e requisiti necessari a proteggere e tutelare le informazioni, siano esse gestite in formato elettronico o cartaceo.
In particolare l'obiettivo è quello di garantire:

- **Confidenzialità**: assicurare che l'informazione sia accessibile solamente a coloro che hanno le dovute autorizzazioni;
- **Integrità**: salvaguardare la completezza dell'informazione e delle sue modalità di trasferimento;
- **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni, e agli elementi architetturali associati, quando ne fanno richiesta.

La mancanza di adeguati livelli di sicurezza connessi a tali parametri può generare conseguenze negative per l'azienda. Pertanto, la sicurezza delle informazioni e la tutela dei dati personali è essenziale per garantire l'operatività aziendale e la tutela dei dati personali di dipendenti e clienti.

6.2.1 PRINCIPI FONDAMENTALI DEL CONTROLLO ACCESSI

L’accesso alle informazioni deve rispettare il principio del “need-to-know”, ossia la condivisione, l’accesso e la comunicazione delle informazioni deve essere garantita al solo personale che, preventivamente identificato ed autorizzato per un periodo di tempo determinato, ne ha effettiva necessità per lo svolgimento delle proprie mansioni lavorative.
Nell’ambito del trattamento delle informazioni attraverso sistemi informatici, il controllo degli accessi da parte degli utenti di tali sistemi deve essere realizzato attraverso:

a) **l’identificazione dell’utente** che richiede l’accesso alle informazioni attraverso un identificativo univoco (User ID) preventivamente assegnatogli;

b) **l’autenticazione dell’utente,** ovvero la verifica che l’utente sia effettivamente la persona che dichiara di essere;

c) **l’autorizzazione dell’utente**, ovvero la concessione dell’accesso alle funzionalità e alle informazioni richieste in funzione di un profilo di autorizzazione preventivamente assegnatogli.

La gestione delle utenze deve rispettare i seguenti requisiti di sicurezza in merito alle modalità di **gestione della password**. In particolare è necessario:

- implementare un meccanismo di access control adeguato, che vieti l’accesso a quanto non espressamente permesso;
- non assegnare alcun privilegio/permesso all’utente fin quando il processo di autenticazione e autorizzazione non è stato completato;
- La procedura di accesso e log-on dell’applicazione deve ridurre al minimo le informazioni fornite agli utenti non ancora autenticati e prevedere la modifica obbligatoria della password iniziale al primo utilizzo;
- prevedere il cambio periodico della password da parte dell’utente;
- prevedere meccanismi automatici di blocco dell’utenza a seguito di un numero limitato di tentativi di accesso negato;
- mascherare i caratteri della password durante la digitazione;
- impedire accessi non autorizzati ai sistemi di gestione delle utenze e delle relative password.

Inoltre, tutti gli accessi ai sistemi informatici devono essere tracciati mediante file di log degli accessi.
Il file di log degli accessi deve riportare le seguenti informazioni minime:

- data e ora dell'accesso o del tentativo di accesso;
- data e ora della disconnessione;
- l’identificativo dell’account cui si riferisce l’accesso;
- l'identificativo del sistema di elaborazione e della componente software cui si riferisce l’accesso.

Con riferimento agli amministratori di sistema, oltre agli accessi ai sistemi informatici, devono essere tracciate le attività svolte su di essi mediante file di log delle attività.
In particolare, le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono 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, in accordo con quanto previsto dal provvedimento del Garante del 27 novembre 2008.

6.2.2 PRINCIPI FONDAMENTALI DELLA GESTIONE DELLE UTENZE

L'intero ciclo di vita delle abilitazioni di accesso ai sistemi informatici (creazione di account utente, modifica account utente e la rimozione dell'account utente), deve essere definito e formalizzato in modo da ridurre il rischio di accesso non autorizzato alle informazioni e ai dati personali.
In particolare, al processo di gestione delle utenze sono applicabili i seguenti principi:

- **Univocità e tracciabilità**: ogni utenza deve essere assegnata nello stesso periodo di tempo ad un solo utente e deve essere conservata l'informazione, anche storica, relativa a tale assegnazione, inclusi i dati necessari all'identificazione dell'utente. In altri termini, deve sempre essere possibile risalire in maniera certa alla persona fisica assegnataria, in un dato periodo, dell'utenza in oggetto. Inoltre, le utenze standard devono essere assegnate ad un solo utente: non sono cioè riassegnabili, in periodi distinti, a diversi utenti;
- **Minimo Privilegio**: i privilegi concessi ad ogni utente devono consentire l'accesso ai soli dati necessari per lo svolgimento delle attività richieste dal proprio ruolo organizzativo;
- **Separazione dei ruoli**: le attività considerate critiche devono essere separate a livello operativo per evitare quanto più possibile che lo stesso utente possa portare a compimento un intero processo critico in autonomia.

Il processo di gestione delle utenze deve prevedere le seguenti macro-attività operative, al fine di minimizzare il rischio di accesso non autorizzato alle informazioni e ai dati personali:

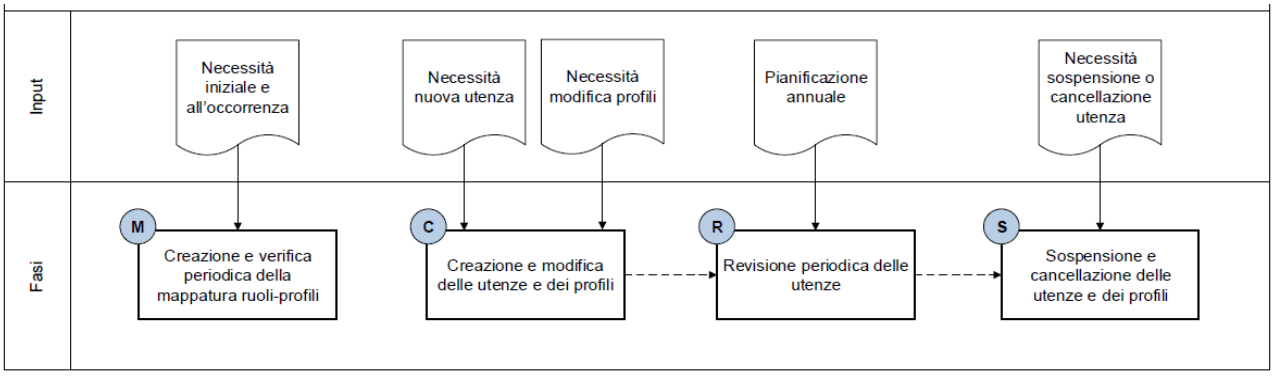
- **Creazione e modifica delle utenze e dei profili**: formalizzazione e verifica della richiesta di concessione di utenze o di modifica dei profili preventivamente definiti nella politica di gestione delle utenze, e il successivo rilascio delle opportune credenziali e privilegi di accesso;
- **Verifica periodica della mappatura ruoli – profili**: verifica periodica dei profili di accesso;
- **Revisione periodica delle utenze**: verifica delle condizioni che giustificano l'assegnazione delle utenze e dei relativi profili di accesso, identificazione di anomalie ed eventuali problematiche e attuazione di eventuali azioni;
- **Sospensione e cessazione delle utenze e dei profili**: sospensione delle utenze e revoca dei profili e cancellazione logica delle utenze e dei relativi profili.

6.3 ANONIMIZZAZIONE E PSEUDONIMIZZAZIONE

L'applicazione di tecniche di anonimizzazione, crittografia e preudonimizzazione ha l'obiettivo di 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. In particolare, la Società, a seconda del rischio associato al trattamento e alla tipologia del dato trattato, dovrà valutare la necessità di adottare una delle seguenti tecniche:

- **Anonimizzazione:** tecnica che si applica ai dati personali al fine di ottenere una de
id
en
tificazione irreversibile del soggetto a cui l'informazione si riferisce;

Figura 7: Processo di gestione delle utenze



- **Crittografia:** si tratta del processo di conversione di un testo in un formato, codificato in modo ermetico, chiamato testo cifrato, che non potrà essere interpretato senza un processo di riconversione al formato originale. Solo la persona autorizzata può decriptare i dati e accedere alle informazioni nel formato originale;
- **Pseudonimizzazione:** tecnica che consente di conservare i dati personali di un soggetto senza che questi siano immediatamente riconducibili ad esso.

La Società dovrà adottare un approccio omogeneo articolato nelle seguenti fasi:

1) **Identificazione dei canali trasmissivi** (es. reti di comunicazione**) e degli ambienti** dove risiedono i dati (es. database, applicativi);
2) **Identificazione dei dati** che devono essere criptatati, anonimizzati, pseudonimizzati (es. nome e cognome, luogo di nascita etc.);
3) **Identificazione delle tecniche** di anonimizzazione / pseudonimizzazione da utilizzare;
4) **Implementazione, monitoraggio e controllo periodico** delle misure adottate.

Si riportano di seguito i principi fondanti e le principali tecniche di anonimizzazione e pseudonimizzazione.

6.3.1 PRINCIPI FONDAMENTALI DELLA PSEUDOMINIZZAZIONE

Il GDPR, all'art. 4 definisce la pseudonimizzazione come il trattamento dei dati personali in modo tale che i dati non possono essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, e a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire la non attribuzione a una persona identificata o identificabile. In altri termini, la tecnica di pseudonimizzazione, consente di conservare i dati personali di un soggetto senza che questi siano immediatamente riconducibili ad esso (interruzione momentanea) e di rendere il soggetto identificabile solo attraverso l'utilizzo delle apposite chiavi di reidentificazione, possedute normalmente solo dal titolare e/o dal responsabile o dall'incaricato appositamente designato (interruzione selettiva).

L'applicazione della pseudonimizzazione ai dati personali permette quindi al titolare del trattamento di effettuare un trattamento legittimo e di ridurre le minacce alla sicurezza dei dati degli interessati (come evidenziato dall'art. 32 comma 1 del GDPR).

Viene riportato di seguito un elenco esemplificativo e non esaustivo delle principali tecniche di pseudonimizzazione che la Società potrà adottare per mitigare i rischi identificati in fase di valutazione di impatto:

- **Crittografia:** si tratta del processo di conversione di un testo in un formato, codificato in modo ermetico, chiamato testo cifrato, che non potrà essere interpretato senza un processo di riconversione al formato originale. Ipotizzando di applicare un sistema di crittografia avanzato, la decriptazione può avvenire solamente se si è a conoscenza della chiave. In particolare tra le forme di crittografia più utilizzate vi sono:
    - Cifratura a chiave simmetrica
    - Cifratura a chiave asimmetrica
    - Cifrature a curve ellittiche
- **Funzioni di hash:** corrisponde a una funzione che, a partire da un'immissione di dati di qualsiasi dimensione (l'immissione potrebbe essere costituita da un unico attributo o da un insieme di attributi), restituisce comunque un'emissione di dimensione fissa.

- **Tokenizzazione:** tecnica derivata dalle precedenti in quanto si basa tipicamente sull'applicazione di un meccanismo di crittografia univoca o sull'assegnazione, tramite una funzione indicizzata, di un numero sequenziale o di un numero generato casualmente che non deriva matematicamente dai dati originali.

6.3.2 PRINCIPI FONDAMENTALI DELL'ANONIMIZZAZIONE

L'anonimizzazione, consiste in una tecnica che si applica ai dati personali al fine di ottenere una deidentificazione irreversibile del soggetto a cui l'informazione si riferisce. In altri termini, impedisce a tutte le parti di identificare una persona in un insieme di dati, di collegare due dati all'interno di un insieme di dati (o tra due insiemi distinti di dati) e di dedurre informazioni da tale insieme di dati.
I dati personali devono essere raccolti e trattati in un formato identificabile e, attraverso un "trattamento successivo", si procede alla loro anonimizzazione.
Viene riportato di seguito un elenco esemplificativo e non esaustivo delle principali tecniche di anonimizzazione che la Società potrà adottare per mitigare i rischi:

1. **Randomizzazione**: famiglia di tecniche che modifica la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona. Se i dati sono sufficientemente incerti non possono più essere riferiti a una persona specifica. Di per sé la randomizzazione non riduce l'unicità di ogni dato, in quanto ciascun dato può comunque essere ancora estrapolato da un'unica persona interessata, ma può rappresentare una tutela dagli attacchi/rischi di deduzione e può essere affiancata da tecniche di generalizzazione per fornire maggiori garanzie di tutela della sfera privata.
2. **Generalizzazione:** consiste nel generalizzare, o diluire, gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (per esempio, una regione anziché una città, un mese anziché una settimana). Sebbene possa essere efficace per impedire l'individuazione, la generalizzazione non consente un'anonimizzazione che risulti efficace in tutti i casi; in particolare, presuppone approcci quantitativi specifici e sofisticati per impedire la correlabilità e la deduzione.

6.4 DATA RETENTION

Con riferimento alla data retention, secondo quanto previsto dal GDPR, è necessario che la Società provveda a definire le tempistiche per la conservazione dei dati personali dei soggetti interessati al trattamento, così che venga garantita la c.d. Deletion By Default richiesta al titolare del trattamento dall'art. 17 del GDPR, oltre che dall'art. 5, paragr. 1, lett. e).

6.4.1 PRINCIPI FONDAMENTALI

I titolari del trattamento devono procedere con la cancellazione dei dati personali, ai sensi dell'art. 17 GDPR, in presenza di due sostanziali casistiche:

- **Deletion By Default:** i dati personali devono essere cancellati in caso di:
    - esaurimento delle finalità per i quali sono stati raccolti;
    - obblighi di legge relativi alla conservazione dei dati;
    - trattamento (a monte) illecito.
- **Deletion On Demand:** i dati personali devono essere cancellati, su richiesta dell'interessato, in quanto:

- revoca il consenso su cui si basa il trattamento, e non sussiste altro fondamento giuridico per il trattamento;
- si oppone al trattamento, e non sussiste altro fondamento giuridico per il trattamento o motivi legittimi prevalenti della Società;
- trattamento (a monte) illecito.

Nella presente Policy tratteremo solamente la deletion by default, mentre con riferimento alla deletion on demand si rimanda alla "Procedura per la gestione dei diritti degli interessati" adottata dalla Società.

La Società non è obbligata a cancellare i dati personali dei suoi interessati, ai sensi dell'art. 17 GDPR, qualora il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione (c.d. diritto di cronaca);
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dalla normativa nazionale o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nella misura in cui il diritto alla cancellazione 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.

6.4.2 PERIODO DI CONSERVAZIONE

Le politiche inerenti i termini di conservazione non sempre sono stabilite normativamente, al contrario per taluni trattamenti è necessario procedere ad un'attenta verifica che il risultato contemperi l'interesse aziendale a conservare i dati, con i principi fissati dal Garante e dal GDPR anche rispetto alle finalità di trattamento perseguite.
Fondamentale in questo ambito risulta essere la mappatura dei trattamenti effettuata tramite il registro dei trattamenti, al fine di comprendere se esistono delle specifiche prescrizioni per quanto riguarda la conservazione dei dati in materia di:

- Normativa in materia commerciale;
- Normativa in ambito tributario/fiscale;
- Normativa in riferimento a diritto del lavoro;
- Normativa in materia di adempimenti amministrativi;

La presente policy di data retention dovrà essere messa a disposizione di tutto il personale attraverso la pubblicazione nella intranet e/o nella bacheca aziendale, o comunque la Società, in qualità di titolare del trattamento, deve essere in grado di dimostrare l'avvenuta conoscenza delle stesse. Il documento dovrà essere tenuto aggiornato alla luce di eventuali modifiche agli obblighi di utilizzo legali o contrattuali.

6.4.3 CRITERI DI CONSERVAZIONE

Il periodo di conservazione dei dati è legato a tre criteri che devono essere presi in considerazione congiuntamente per poter determinare il corretto periodo di retention.

Tali criteri sono:

1. **Categoria di interessati**: sono i soggetti - persone fisiche[5] - cui si riferiscono i dati personali.
   All'interno della Società sono presenti le seguenti categorie:
   - Clienti
   - Dipendenti
   - Collaboratori
   - Candidati
   - Familiari
   - Fornitori
   - Soggetti terzi

2. **Categoria di dati personali**: sono i dati personali trattati nel contesto delle attività del titolare all'interno della Società sono presenti le seguenti categorie:
   - Dati personali comuni
   - Dati giudiziari
3. **Trattamento:** sono le operazioni compiute dalle diverse direzioni e processi della Società sui dati personali dei propri interessati, e si riferiscono alle diverse finalità per le quali vengono trattati.

Si evidenzia come la "*Matrice Data Retention*" (Allegato 1 - Matrice Data Retention) sarà strutturata in funzione della tipologia di interessato, così da poter correttamente orientare la compilazione del "registro dei trattamenti", in caso di nuovo trattamento e/o di revisione/aggiornamento/modifica di un trattamento già in corso. Il periodo di conservazione dei dati come declinato nell'allegato 1 dovrà essere applicato sui singoli trattamenti.

Ogni variazione al periodo di retention sul singolo trattamento/tipologia di interessato dovrà essere recepita nel registro dei trattamenti della Società.

Si precisa che in caso di disaccordo tra i termini di conservazione indicati nella presente Data Privacy Policy e quelli indicati nella singola scheda di trattamento del registro, prevarrà il termine indicato nella singola scheda solamente a fronte di uno specifico razionale che non sia incompatibile con il

presente documento o con la normativa cogente, ovvero venga rimesso ad una specifica DPIA.

6.4.4 PARAMETRI PER LA CANCELLAZIONE/ANONIMIZZAZIONE

Qualora sui medesimi dati personali insistano più prescrizioni normative e/o più finalità che prevedono termini differenti di conservazione, i dati non devono essere cancellati fin quando non sia trascorso il termine di retention della durata maggiore; tuttavia, i dati non potranno più essere trattati per le finalità ormai esaurite, ma unicamente per le finalità che ne giustificano ancora la conservazione (a titolo esemplificativo, i medesimi dati identificativi che dovrebbero essere cancellati per il trattamento di profilazione rimangono conservati - e trattati - esclusivamente per ulteriori lecite finalità).

Qualora i dati siano trattati per una finalità per la quale non è prevista una specifica fonte normativa/regolamentare, la Società stabilisce uno specifico termine per la conservazione di tali

[5] Le persone giuridiche non sono tutelate dal GDPR, come affermato chiaramente dal Considerando 14 "*È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei 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.*"

dati, in base ad un criterio di necessità degli stessi in relazione alla finalità per la quale sono stati acquisiti.

È inoltre prevista la possibilità offerta dal GDPR di sostituire la cancellazione con l'anonimizzazione dei dati[6], pertanto la Società si riserva la possibilità di procedere in tal senso allo scadere dei termini di conservazione previsti ai paragrafi successivi, onde poter compiere analisi o studi statistici su dati non più riconducibili, direttamente o indirettamente, a persone fisiche identificate o identificabili

6.4.5 MATRICE DI DATA RETENTION

Alla presente policy si allega la *Matrice di Data Retention* (Allegato 1 – Matrice Data Retention) la quale riporta i dati mappati all'interno del registro dei trattamenti della Società. Nella matrice sono definite le tempistiche per la conservazione dei dati personali dei soggetti interessati al trattamento, così che venga garantita la c.d. Deletion By Default.

6.5 TRASFERIMENTO DI DATI EXTRA UE

6.5.1 AMBITO DI APPLICAZIONE DEL GDPR

In particolare, ai sensi dell'art. 3 del GDPR, rubricato "Ambito di applicazione territoriale", *il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento* ***nell'Unione****, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.* Pertanto, gli Stati non facenti parte dell'Unione non sono soggetti al rispetto delle disposizioni previste dal Regolamento e, di conseguenza, il livello di sicurezza, di garanzia e di tutela dei dati personali può non corrispondere e non equivalere a quello europeo.

6.5.2 PRINCIPI FONDAMENTALI

Il legislatore europeo, considerata la crescita di flussi transfrontalieri di dati, ovvero di trasferimenti di dati personali verso destinatari soggetti a una giurisdizione differente da quella europea, e per garantire comunque un livello di sicurezza adeguato, impone con gli artt. 44 e seguenti del GDPR determinate condizioni affinché un trasferimento di dati verso paesi terzi possa essere effettuato.
In particolare, ai sensi dell'art. 44 del GDPR:
*"Qualunque trasferimento di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo verso un altro paese terzo, ha luogo solamente se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni [previste dal Regolamento] … **al fine di assicurare che il livello di protezione delle persone fisiche garantito dal GDPR non sia pregiudicato**".*
Il trasferimento dei dati personali dell'Interessato in paesi diversi da quello di raccolta può avvenire, ad esempio, nei seguenti casi:

1. **se trasferimento dei dati personali si basa sul consenso** espresso dell'interessato e, se si tratta di dati particolari, in forma scritta;
2. **se trasferimento risulta essere necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato** o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

[6] Considerando 26 del GDPR: *"(…) I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire 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. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca."*

3. **se trasferimento è necessario ai fini dello svolgimento delle investigazioni difensive** di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
4. **se trasferimento avviene verso paesi che garantiscano un adeguato livello di protezione dei dati personali.** In particolare, ai sensi dell'art. 45 del GDPR, il trasferimento è ammesso e non necessita di autorizzazioni specifiche se la Commissione, mediante atti di esecuzione, decide che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato (Decisione di adeguatezza sul livello di protezione); La valutazione di adeguatezza deve tener conto di precisi elementi espressamente previsti dall'art. 45 comma 2 del GDPR. Deve essere poi svolto un riesame periodico di tale decisione almeno ogni quattro anni, al fine di mantenere sotto controllo l'effettiva esistenza di un livello di protezione adeguato in linea con quanto previsto dalla normativa. Tali decisioni della Commissione devono essere pubblicate nella Gazzetta Ufficiale dell'UE e pubblicate sul sito della Commissione europea stessa;
5. **se il trasferimento è soggetto ad adeguate garanzie**. In particolare, ai sensi dell'art. 46 del GDPR, il titolare o il responsabile del trattamento possono trasferire dati personali verso un paese terzo solo se hanno fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Possono considerarsi garanzie adeguate ai sensi dell'art. 46 comma 2 le norme vincolanti di impresa, le clausole contrattuali standard adottate dalla Commissione o dalle autorità di controllo, codici di condotta o certificazioni;
6. **se il trasferimento avviene tra società facenti parte dello stesso gruppo d'impresa** mediante norme vincolanti d'impresa (BCR – Binding Corporate Rules). Le BCR consistono in una serie di clausole contrattuali che dettano principi (in linea con il GDPR e che assicurano un livello di protezione adeguato) vincolanti per tutte le società facenti parte del gruppo. Le BCR devono essere esaminate e approvate dall'autorità di controllo nazionale o europea che deve verificare la sussistenza dei contenuti minimi espressamente previsti dall'art. 47 del GDPR.

Da ultimo, lo stesso art. 49 del GDPR stabilisce che il trasferimento verso paesi extra UE è ammesso solo se non è ripetitivo, se riguarda un numero limitato di interessati ed è necessario per il perseguimento di interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. In tali occasioni il titolare informa comunque l'autorità di controllo e, oltre all'informativa "standard", mette a conoscenza l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.
In conclusione, al di fuori di tali situazioni ordinarie ed eccezionali citate, il trasferimento dei dati personali verso Paesi terzi non è mai consentito.

7 ISPEZIONI DA PARTE DEL GARANTE E SANZIONI

7.1 ISPEZIONI DA PARTE DEL GARANTE

Il Garante e altre autorità di vigilanza competenti possono effettuare ispezioni presso la Società, al fine di verificare la compliance con i requisiti del GDPR.

Gli incaricati dovranno prestare la massima collaborazione ai funzionari dell'autorità di vigilanza che effettuino le suddette ispezioni e fornire tutte le informazioni attinenti alle operazioni di trattamento di dati personali svolte che siano richieste dagli stessi.

7.2 SANZIONI

La violazione della normativa in materia di protezione dei dati personali può esporre il titolare a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale) a seconda delle norme concretamente violate ed avere sulla Società impatti reputazionali negativi, anche rilevanti. L'accertamento di determinate violazioni può anche comportare l'emissione, da parte delle autorità competenti, di ordini finalizzati alla cancellazione dei dati personali raccolti o all'interruzione di determinate operazioni di trattamento che si assumono illecite. Inoltre, gli interessati possono promuovere azioni di risarcimento per i danni subiti a causa dello svolgimento di operazioni di trattamento, riguardanti i loro dati personali, non conformi alla normativa.

8 FORMAZIONE

Gli interventi formazione hanno l'obiettivo di rendere edotti gli incaricati al trattamento dei rischi che insistono sui dati personali, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina della protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

L'attività di formazione è organizzata dal Referente Data Protection e dalla Funzione Risorse Umane: la stessa dovrà essere erogata al personale entro un periodo ragionevolmente breve dal momento dell'ingresso in servizio, nonché in caso di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

I contenuti essenziali della formazione dovranno essere i seguenti:

- ambiti legislativi, adeguamento alla normativa ed ai provvedimenti del Garante;
- tipologia di dati e modalità di trattamento degli stessi;
- modello di gestione data protection implementato;
- ruoli previsti per il trattamento dei dati personali;
- informativa e consenso, diritti di accesso, reclami e sanzioni;
- le misure di sicurezza adottate.

9 AUDIT

La Funzione Internal Audit svolge attività di audit sul processo di gestione degli adempimenti data protection, con l'obiettivo di rilevare lo stato di conformità rispetto alla normativa, ai provvedimenti, alla regolamentazione di settore applicabile ed alle disposizioni contenute nel presente documento.

Le verifiche hanno ad oggetto i trattamenti svolti dalla Società e possono riguardare, ove necessario, anche le attività svolte da soggetti esterni nominati (es. Responsabili del trattamento).

Inoltre, la suddetta struttura organizzativa può effettuare verifiche previste in conformità alla normativa applicabile agli amministratori di sistema, volte ad acquisire presso la struttura organizzativa i log di accesso (sia quelli di login che quelli di logout) di tutti i sistemi contenenti dati personali al fine di verificare l'aderenza del loro operato alle misure organizzative, tecniche e di sicurezza per il trattamento dei dati personali previste dalle norme vigenti.

In particolare sono verificate le anomalie nella frequenza degli accessi e nelle loro modalità, ad esempio: orari, durata, sistemi cui si è fatto accesso. Ulteriori attività di controllo riguardano l'esecuzione di verifiche a campione sulla documentazione (lista degli Amministratori di Sistema, lettere di nomina, relazioni d'idoneità) relativamente agli adempimenti formali in materia di Amministratori di Sistema.

Altre verifiche riguardano le attività degli incaricati alla videosorveglianza che devono essere eseguite con cadenza periodica al fine di verificare l'applicazione dei requisiti normativi e dell'applicazione della presente Data Privacy Policy.

10 ALLEGATI

10.1 ALLEGATO 1 - MATRICE DATA RETENTION

Viene di seguito riportata la Matrice Data Retention, la quale riporta i dati mappati all'interno del registro dei trattamenti della Società
Nella matrice sono definite a seconda della tipologia di dato trattato le tempistiche per la conservazione dei dati personali dei soggetti interessati al trattamento, così che venga garantita la c.d. Deletion By Default.

Categoria di dato trattato	Periodo di conservazione	Note
Dati personali comuni	• I dati personali oggetto di trattamento devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati. Pertanto, ogni azienda, società o altro tipo di ente dovrà adeguarsi a tale previsione normativa, provvedendo senza ritardo alla cancellazione o alla anonimizzazione dei dati nel momento in cui la conservazione dei dati personali non risulti ulteriormente giustificata. • I dati personali relativi al fascicolo dipendente (anagrafica, qualifica, contratto applicato, retribuzione base, infortuni, calendario delle presenze, dati relativi alle performance, dati relativi alla formazione) devono essere conservati: - per 5 anni dalla registrazione nel LUL; - per 10 anni dalla cessazione del rapporto di lavoro (ad eccezione dei dati necessari ad assicurare la tutela della Società in sede giudiziale in caso di contenzioso). In particolare in caso di contenzioso tra la società e il dipendente circa la cancellazione di alcuni dati di quest'ultimo, il Garante (Provvedimento Garante del 23 dicembre 2010) ha riconosciuto il diritto dell'impresa di conservare i file del dipendente al fine di poterli eventualmente presentare come prova nell'ambito del contenzioso penale. L'acquisizione dei dati nel procedimento dovrà comunque avvenire su precisa disposizione del giudice. • I dati relativi ai mancati pagamenti dovranno essere conservati unicamente per un periodo di 90 giorni (tempo necessario per il rimborso), al termine di tale periodo i dati dovranno essere cancellati.	• Art.11, comma 1, lett. e) del Codice della Privacy

Categoria di dato trattato	Periodo di conservazione	Note
Dati sensibili	**Dati sensibili nei rapporti di lavoro.** In questo caso possono essere conservati per un periodo non superiore a quello necessario per adempiere ai seguenti obblighi o ai seguenti compiti: 1. per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro; 2. ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori; 3. per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo; 4. per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi; 5. per esercitare il diritto di accesso ai dati e ai documenti amministrativi 6. per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali. 7. per garantire le pari opportunità nel lavoro; 8. per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.	• Autorizzazione n. 1/2016 - Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro - 15 dicembre 2016

Categoria di dato trattato	Periodo di conservazione	Note
Dati giudiziari	Non sono previste prescrizioni normative in merito alla conservazione dei dati giudiziari. Tuttavia, secondo quanto previsto dal GDPR, è necessario definire un termine di conservazione dei dati congruo e non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento. In particolare i dati personali devono essere: "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);"*	• Considerando 39 del GDPR • Articolo 5 comma 1 lettera e del GDPR

Categoria di dato trattato	Periodo di conservazione	Note
Dati di videosorveglianza	• Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita. La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana. Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione". In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.	• Provvedimento in materia di videosorveglianza - 8 aprile 2010

10.2 ALLEGATO 2 – MISURE BY DESIGN

La Società dovrà adottare le opportune misure tecniche di sicurezza, considerate come adeguate rispetto al contesto, alla natura, all'oggetto e alle finalità del nuovo trattamento/progetto, tenendo a riferimento le seguenti categorie di misure:

- **Vulnerability Assessment & Penetration Testing:** applicazione di procedure sistematiche di verifica delle vulnerabilità presenti nelle applicazioni in uso nella Società;
- **Patch Management:** verifica ed applicazioni delle patch di sicurezza necessarie per i sistemi e le applicazioni in uso nella Società;
- **Malware Protection:** protezione da infezioni di software malevolo, difesa da azioni non autorizzate di applicazioni sospette e protezione da tentativi di sottrazione di dati personali;
- **Meccanismi di identificazione e autenticazione:** meccanismi di identificazione e autenticazione e meccanismi per il controllo centralizzato degli accessi;
- **Utilizzo di utenze nominative:** sui sistemi sono previste solo utenze nominative (evitando account generici o di gruppo) per garantire la tracciabilità delle operazioni svolte;
- **Password Policy:** L'accesso ai sistemi avviene mediante user id e password conforme ai criteri minimi di sicurezza;
- **Meccanismi di autorizzazione:** l'assegnazione dei profili a sistema avviene nel rispetto dei principi di "segregation of duties" e "least privilege": i permessi ("grant") sui sistemi sono assegnati agli utenti sulla base delle richieste dei rispettivi responsabili con un'analisi di eventuali conflitti di segregazione dei ruoli effettuata congiuntamente con il business;
- **Data Encryption/anonymization/pseudonymization:** adozione di meccanismi di cifratura, anonimizzazione e pseudonimizzazione per la protezione dei dati personali e confidenziali;
- **Security Event Management & Log Management:** presenza di sistemi di gestione e memorizzazione centralizzata di eventi e log provenienti dai servizi di monitoring presenti nella rete sottoposta al controllo;
- **Incident & Data Breach Management:** procedure di individuazione, contenimento e risoluzione di situazioni di rischio per la sicurezza dei dati e dei sistemi informativi in fase post-intrusione.

10.2.1 TABELLA DI DETTAGLIO MISURE BY DESIGN

ID	Categoria di misura	Riferimenti		Descrizione
		GDPR	Standard di Sicurezza (SANS 20 Critical Security Controls; ISO-IEC 27001/13; NIST SP 800-53)	
1	**Vulnerability Assessment & Penetration Testing**	Art. 32	SANS/CSC 04 SANS/CSC 20 NIST/CA-2 NIST/RA-3 NIST/RA-5 NIST/SI-2 NIST/SI-5 ISO 27001/A.12.6.1 ISO 27001/A.14.2.8 Allegato "B" al D.Lgs. 196/03 punto 17	Applicazione di procedure sistematiche di verifica delle vulnerabilità presenti nelle applicazioni in uso nella Società.
2	**Patch Management**	Art. 32	SANS/CSC 04 SANS/CSC 20 NIST/CA-2 NIST/RA-3 NIST/RA-5 NIST/SI-2 NIST/SI-5 ISO 27001/A.12.6.1 ISO 27001/A.14.2.8 Allegato "B" al D.Lgs. 196/03 punto 17	Verifica ed applicazioni delle patch di sicurezza necessarie per i sistemi e le applicazioni in uso nella Società.
3	**Malware Protection**	Art. 32	SANS/CSC 13 SANS/CSC 10 NIST/SI-3 ISO 27001/A.12.2 Allegato "B" al D.Lgs. 196/03 punto 17	Protezione da infezioni di software malevolo, difesa da azioni non autorizzate di applicazioni sospette e protezione da tentativi di sottrazione di dati personali.

ID	Categoria di misura	Riferimenti		Descrizione
		GDPR	Standard di Sicurezza (SANS 20 Critical Security Controls; ISO-IEC 27001/13; NIST SP 800-53)	
4	**Meccanismi di identificazione e autenticazione**	Art. 32	SANS/CSC 05 SANS/CSC 14 SANS/CSC 16 NIST/AC-1 NIST/AC-2 NIST/AC-20 NIST/IA-1 ISO 27001/A.9.2 Allegato "B" al D.Lgs. 196/03 punti da 2 a 9	Sono previsti dei meccanismi di identificazione e autenticazione e meccanismi per il controllo centralizzato degli accessi.
5	**Utilizzo di utenze nominative**	Art. 32	SANS/CSC 05 SANS/CSC 14 SANS/CSC 16 NIST/AC-1 NIST/AC-2 NIST/AC-20 NIST/IA-1 ISO 27001/A.9.2 Allegato "B" al D.Lgs. 196/03 punti da 2 a 9	Sui sistemi sono previste solo utenze nominative (evitando account generici o di gruppo) per garantire la tracciabilità delle operazioni svolte.
6	**Password Policy**	Art. 32	SANS/CSC 05 SANS/CSC 14 SANS/CSC 16 NIST/AC-1 NIST/AC-2 NIST/AC-20 NIST/IA-1 ISO 27001/A.9.2 Allegato "B" al D.Lgs. 196/03 punti da 2 a 9	L'accesso ai sistemi avviene mediante user_id e password conforme ai criteri minimi di sicurezza.

ID	Categoria di misura	Riferimenti		Descrizione
		GDPR	Standard di Sicurezza (SANS 20 Critical Security Controls; ISO-IEC 27001/13; NIST SP 800-53)	
7	**Meccanismi di autorizzazione**	Art. 32	SANS/CSC 05 SANS/CSC 14 SANS/CSC 16 NIST/AC-1 NIST/AC-2 NIST/AC-20 NIST/IA-1 ISO 27001/A.9.2 Allegato "B" al D.Lgs. 196/03 punti da 2 a 9	L'assegnazione dei profili a sistema avviene nel rispetto dei principi di "segregation of duties" e "least priviledge": i permessi ("grant") sui sistemi sono assegnati agli utenti sulla base delle richieste dei rispettivi responsabili con un'analisi di eventuali conflitti di segregazione dei ruoli effettuata congiuntamente con il business.
8	**Data Encryption**	Art. 32 Art. 34	SANS/CSC 13 NIST/AC-17 NIST/SC-8 NIST/SC-13 ISO 27001/A.13.1 ISO 27001/A.14.1.2 ISO 27001/A.14.1.3 Allegato "B" al D.Lgs. 196/03 punto 24 GDPR, Art. 32	Adozione di meccanismi di cifratura per la protezione dei dati personali e confidenziali.
9	**Security Event Management & Log Management**	Art.33, Considerando 49, 87, 88	SANS/CSC 06 NIST/SI-4 ISO 27001/A.12.4	Presenza di sistemi di gestione e memorizzazione centralizzata di eventi e log provenienti dai servizi di monitoring presenti nella rete sottoposta al controllo.
10	**Incident & Data Breach Management**	Art.33, Considerando 49, 87, 88	SANS/CSC 19 NIST/IR-1 NIST/IR-3 NIST/IR-5 NIST/IR-6 ISO 27001/A.6.1.3 ISO 27001/A.16.1.2 ISO 27001/A.16.1.5	Procedure di individuazione, contenimento e risoluzione di situazioni di rischio per la sicurezza dei dati e dei sistemi informativi in fase post-intrusione.

ID	Categoria di misura	Riferimenti		Descrizione
		GDPR	Standard di Sicurezza (SANS 20 Critical Security Controls; ISO-IEC 27001/13; NIST SP 800-53)	
			GDPR, Art. 33	
11	**Business Continuity & Disaster Recovery Management**	Art. 32	SANS/CSC 10 - Partially NIST/CP-1 NIST/CP-2 NIST/CP-10 NIST/CP-13 ISO 27001/A.12.2 ISO 27001/A.6.1.1 ISO 27001/A.17.1.1 ISO 27001/A.17.1.2 ISO 27001/A.17.2.1	Misure di gestione degli eventi avversi alla continuità aziendale e salvaguardia delle attività produttive.
12	**Network Protection (IDS, IPS, Firewall, URL Filtering, network segmentation)**	Art. 32	SANS/CSC 07 SANS/CSC 08 SANS/CSC 09 SANS/CSC 11 SANS/CSC 12 SANS/CSC 15 NIST/SC-28 NIST/SI-4 NIST/SC-28 NIST/SI-4 ISO 27001/A.13.1.1 ISO 27001/A.12.3.1 ISO 27001/A.13.1.1 ISO 27001/A.18.1.3 Allegato "B" al D.Lgs. 196/03 punto 16	Progettazione sicura della infrastruttura di rete dei sistemi informativi e protezione da accessi di rete non autorizzati.

ID	Categoria di misura	Riferimenti		Descrizione
		GDPR	Standard di Sicurezza (SANS 20 Critical Security Controls; ISO-IEC 27001/13; NIST SP 800-53)	
13	**Data Loss Prevention**	Art. 32	SANS/CSC 13 SANS/CSC 06 NIST/CP-9 NIST/SC-28 ISO 27001/A.18.1.3	Procedimenti di prevenzione di rilascio/perdita di dati sensibili esternamente al perimetro del sistema informativo.
14	**Backup & Restore**	Art. 32	NIST/CP-9 ISO 27001/A.12.3 ISO 27001/A.17.1.2 ISO 27001/A.18.1.3 Allegato "B" al D.Lgs. 196/03 punto 18	Adozione di misure per la memorizzazione e il recupero di dati duplicati a garanzia della continuità aziendale.
15	**Registrazione degli accessi degli Amministratori di Sistema**	/	Provvedimento Generale del Garante del 27 novembre 2008	Gli accessi degli Amministratori di Sistema agli archivi elettronici sono registrati mediante log di sistema e conservati per un periodo di tempo di almeno 6 mesi. I log possiedono le caratteristiche minime richieste (username, host, IP, data e ora di log-in e log-out).