# SI - GDPR SIstema di gestione del GDPR

**VERSIONE 1.2 - Aprile 2019**
*da Gennaio 2019 sostituisce in versione WIKI precedenti versioni PDF aggiornate fino a Novembre 2018*

**Table of Contents [-]**



## Premessa

Il presente documento illustra le attività operative che Intesys e Intesys Openway pongono in essere per assicurare la compliance Vs. il Regolamento (UE) 679/2016 in materia di protezione dei dati personali (nel seguito "il Regolamento").

Le attività organizzative, procedurali e tecnologiche riportate nei paragrafi successivi sono state definite in base a:

- Le analisi di conformità dell'azienda Vs. il decreto Legislativo 196/2003, denominato "Codice in materia di protezione dei dati personali" (nel seguito anche "Codice Privacy");
- Le analisi di conformità dell'azienda Vs. i Provvedimenti del Garante della Privacy applicabili allo specifico contesto aziendale, ovvero:
  - G.U. n. 300 del 24 dicembre 2008 - Attribuzioni delle funzioni di amministratore di sistema;
  - G.U. n. 99 del 29 aprile 2010 - Videosorveglianza;
  - G.U. n. 126 del 3 giugno 2014 - Informativa e consenso per l'uso dei cookies;
  - G.U. n. 58 del 10 marzo 2007 - Posta elettronica e internet.
  - G.U. n. 287 del 9 dicembre 2008 - Rifiuti di apparecchiature elettriche ed elettroniche.

Le attività operative di cui al presente documento sono estese anche alla controllata Intesys Openway, secondo le modalità man mano dettagliate nel testo.

## Contesto aziendale

### Estremi dell'organizzazione

Intesys s.r.l. - P.IVA 02601270230
Intesys Openway s.r.l. - P.IVA 04191640236
operanti entrambe nella stessa sede in Via Roveggia 122/a, 37136 Verona - tel. +39 045 503663 - fax +39 045 503604

### Prodotti e servizi

INTESYS S.r.l. e INTESYS OPENWAY (nel seguito, quando opportuno, "Azienda" o "Aziende") operano sul territorio nazionale come Technological Digital Agency nel settore del design, sviluppo e gestione di progetti di Digital Marketing, Brand Site, E-Commerce, Software Enterprise e System Integration, Document Management, Business Process Management. Scopo istituzionale delle Aziende è la realizzazione soluzioni digitali avanzate attraverso l'integrazione di competenze strategiche di marketing digitale e tecnologiche, per offrire ai propri Clienti un vantaggio competitivo derivante da un'efficace ed efficiente gestione delle relazioni digitali. Alcuni dei servizi offerti dall'Azienda sono:

- Progettazione e sviluppo di portali dedicati;
- Sistemi di prenotazione e pagamento On-Line;
- Gestione di processi aziendali attraverso Intranet collaborative;
- Gestione dell'Identity Management attraverso architetture di Single Sign On;
- Sviluppo software negli ambienti Liferay, Magento e Ruby On Rails;
- Consulenza e sviluppo di progetti di Business Process Management.
- Consulenza e sviluppo di progetti di gestione documentale
- Elaborazione Digital Strategy, Digital COmmunication e Digital Marketing.

Alla data le Aziende occupano circa 60 dipendenti

### Struttura societaria

Intesys SRL, di proprietà di sei persone fisiche che detengono il 100% delle quote, controlla 2 società: Intesys Networking srl al 100%, Intesys Openway al 70%.

### Intesys Openway

Intesys Openway srl (di seguito, quando opportuno, "Controllata") in particolare opera sul territorio nazionale offrendo soluzioni di workflow management e gestione dei processi documentali, protocollo informatico e ufficio digitale. Ha un organico composto da 4 persone ed è ospitata presso la sede di Intesys srl di cui è controllata al 70%. Quando nel seguito di parla di "sede della Azienda" si intende anche "sede della Controllata".

### Scopo

Si ricorda che il presente documento raccoglie quanto in essere nell'Azienda e relativamente alla Controllata in materia di sicurezza e protezione dei dati personali, in adempimento alle prescrizioni di cui al Regolamento.

Lo scopo del presente documento è quello di delineare il quadro generale delle misure di protezione dei dati personali trattati all'interno del perimetro aziendale o a cura di Responsabili esterni dei trattamenti, identificando le misure di sicurezza delle informazioni e gli adempimenti necessari per garantire l'ottemperanza ai principi di protezione dei dati personali, che il Titolare ha predisposto nel rispetto dei diritti degli interessati.

Il presente documento costituisce, inoltre, uno strumento per garantire la rintracciabilità delle Linee Guida e delle Procedure adottate dall'Azienda e dalla Controllata in materia di sicurezza dei dati personali.

Il presente documento è redatto a cura e sotto la responsabilità del Responsabile Privacy dell'Azienda con il supporto delle Funzioni interessate e approvato dal Titolare.

### Riferimenti ad altra documentazione aziendale

Il Sistema di Gestione del GDPR (di seguito SG-GDPR) è integrato con il Sistema di Gestione della Sicurezza Informatica (di seguito SG-SI) a costituire un sistema di norme e procedure per la sicurezza dell'informazione, in particolare per i dati di natura personale con valenza sia per la Azienda sia per la Controllata.

### Principali definizioni

Dati personali: tutte quelle informazioni, come nome, cognome, partita IVA, codice fiscale, indirizzo (compreso quello di posta elettronica), numeri di telefono, numero patente, che consentono di individuare una persona fisica o giuridica, sia essa anche un ente od associazione.

Dati personali particolari: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale della persona. Rientrano in questa categoria i dati genetici, i dati biometrici e i dati relativi alla salute o alla vita sessuale della persona.

Dati personali relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Altri dati con rischio elevato: dati il cui trattamento può presentare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori) .

Interessato: la persona fisica a cui si riferiscono i dati personali.

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.

Limitazione del trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: 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: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

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 o degli Stati.

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: 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: 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.

## Limiti di validità

Le norme e le procedure contenute nel SG-GDPR sono applicabili a tutte le attività di trattamento dei dati personali svolte presso la sede dell'Azienda.

## Policy Data Protection

Il presente documento integra e tiene in considerazione il SG-SI adottato dalla Azienda e valido anche per la Controllata .

### Ambito di applicazione della policy

La presente policy è applicata alle informazioni e ai dati specificati nel paragrafo "Tipologie di informazioni" contenuto nel SG-SI e al personale che collabora a titolo continuativo con l'Azienda e la Controllata.

### Commitment

Il Management di INTESYS S.r.l. pone la massima attenzione alla sicurezza del patrimonio informativo aziendale e alla protezione dei dati personali oggetto di trattamento. La forte sensibilità verso queste tematiche ha permesso ad INTESYS S.r.l. di predisporre e adottare, nel corso del tempo, misure di sicurezza (organizzative e tecniche) coerenti con

- lo Standard ISO 27001:2013 "Information security management systems";
- lo Standard ISO 29151:2017 "Code of practice for personally identifiable information protection";
- il Regolamento (UE) 679/2016 in materia di protezione dei dati personali e le norme collegate;
- Il D.Lgs. 196/2001 intitolato "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018.
- Le norme collegate alle precedenti (es. Provvedimenti del garante della Privacy).

A questo proposito si segnala che, nello svolgimento delle proprie attività, INTESYS S.r.l. effettua il trattamento di dati personali (anche particolari) relativi ai propri dipendenti e ai dipendenti della propria Controllata esclusivamente per finalità connesse alla gestione e all'amministrazione delle risorse umane. Le attività di trattamento sono svolte in virtù delle seguenti condizioni di liceità:

- Svolgimento di un contratto di cui l'Interessato è parte;
- Adempimento di obblighi di legge al quale è soggetto il Titolare.

### Modello organizzativo privacy

Il SG-SI adottato dalla Azienda prevede tutti gli elementi relativi alla organizzazione della sicurezza informatica, ivi inclusi:
- i trattamenti di dati personali oggetto del GDPR,
- le figure di coordinamento,
- compiti, ruoli e responsabilità,
- il piano operativo per la sicurezza fisica,
- il piano operativo per la sicurezza logica,
- il piano operativo per la sicurezza organizzativa,
- la formazione
- le attività di revisione e miglioramento,
- la gestione e protezione degli asset,
- la gestione sistemi ICT,
- la gestione della comunicazione e trasmissione dati,
- lo sviluppo software e manutenzione dei sistemi,
- la gestione della Business Continuity,
- la gestione dei rapporti con Fornitori e Outsourcers,
- le attività di audit.

## Provvedimenti Garante Privacy applicabili e modalità di adozione

1. G .U. n. 300 del 24 dicembre 2008 - Attribuzioni delle funzioni di amministratore di sistema;
1. G .U. n. 99 del 29 aprile 2010 - Videosorveglianza;
2. G.U. n. 126 del 3 giugno 2014 - Informativa e consenso per l'uso dei cookies;
3. G .U. n. 58 del 10 marzo 2007 - Posta elettronica e internet.
4. G .U. n. 287 del 9 dicembre 2008 - Rifiuti di apparecchiature elettriche ed elettroniche.

### Amministratore di Sistema

Riferimenti normativi: G.U. n. 300 del 24 dicembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

Gli Amministratori di Sistema sono formalmente nominati sulla base della loro mansione, della loro competenza e della loro esperienza tecnica. La lettera di nomina ad Amministratore di Sistema (AdS) contiene le seguenti informazioni:
- attestazione dell'incarico;
- elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- indicazione delle "verifiche" periodiche che il Titolare svolgerà sulle attività svolte dall'Amministratore di Sistema (con particolare riferimento all'analisi semestrale dei LOG e alle interviste periodiche sullo svolgimento dell'attività);

Come specificato nel SG-SI, l'Azienda e la Controllata adottano un sistema per la registrazione degli accessi logici ai sistemi di elaborazione da parte degli Amministratori di Sistema.

Inoltre, viene effettuata una puntuale gestione dei LOG degli Amministratori di Sistema che:
- sono resi inalterabili al momento della raccolta attraverso un back-up immediato su sistemi protetti con impossibilità di accesso da parte degli Amministratori di Sistema;
- mantenuti sui sistemi aziendali per un tempo minimo di 6 mesi;
- analizzati periodicamente per individuare eventuali attività illecite.

Ulteriori elementi tecnici sono specificati nel SG-SI e documentazione relativa.

### Videosorveglianza

*Riferimenti normativi: G.U. n. 99 del 29 aprile 2010 - Provvedimento in materia di videosorveglianza.*

L'installazione del sistema di videosorveglianza della Azienda è stata effettuata previo accordo con la Rappresentanza Sindacale Aziendale (o previa autorizzazione del Servizio Ispettivo della Direzione Territoriale del Lavoro).

Viene resa visionabile agli interessati una informativa "estesa" relativa alla raccolta di immagini tramite servizio di videosorveglianza, posizionata agli ingressi della Sede in prossimità del campanello/citofono.

Sono inoltre presenti appositi cartelli di segnalazione della presenza di un sistema di videosorveglianza che riportano le seguenti informazioni minime:
- nome del Titolare del Trattamento;
- finalità del trattamento;
- rimando alla informativa estesa.

Ulteriori misure di sicurezza:
- Il supporto di registrazione collegato al sistema di videosorveglianza è fisicamente protetto da accessi fisici e logici non autorizzati;
- Tutte le registrazioni del sistema di videosorveglianza vengono mantenute per 72 ore;
- Le registrazioni più vecchie sono cancellate con cadenza giornaliera;
- E' predisposto un registro delle attività di manutenzione del sistema di videosorveglianza;
- Nel caso di sostituzione dei dispositivi fisici di memorizzazione viene effettuata una distruzione fisica dei dispositivi.

### Cookies

Riferimenti normativi: G.U. n. 126 del 3 giugno 2014 - Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies.

Nella home page (o altra pagina) del sito Web della Azienda e della Controllata compare immediatamente un pop-up contenente le seguenti indicazioni:
- che il sito utilizza cookie di profilazione;
- che il sito consente anche l'invio di cookie "terze parti" (ove previsto);

- il link all'informativa estesa;
- l'indicazione che alla pagina dell'informativa è possibile negare il consenso all'uso di cookie;
- l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso comporta il consenso all'uso dei cookie.

L'informativa estesa, in particolare:

- descrive in maniera specifica e analitica le caratteristiche e le finalità dei cookie installati dal sito;
- consente all'utente di selezionare/deselezionare i singoli cookie;
- è raggiungibile mediante un link inserito nell'informativa breve, come pure attraverso un riferimento su ogni pagina del sito, collocato in calce alla medesima;
- indica la possibilità per l'utente di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da eseguire per configurare tali impostazioni.

#### Internet e posta elettronica

*Riferimenti normativi: G.U. n. 58 del 10 marzo 2007 - Lavoro: le linee guida del Garante per posta elettronica e internet.*

All'interno del SG-SI sono formalizzate e precisate le regole per il corretto utilizzo di internet e posta elettronica, indirizzando le seguenti tematiche:

- navigazione in Internet;
- scaricamento software;
- partecipazione a forum, chat e piattaforme simili;
- memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria;
- regole di gestione e di uso della posta elettronica aziendale al di fuori delle mansioni di lavoro;
- utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list senza attinenza con l'attività professionale svolta.

#### Smaltimento rifiuti elettronici

Riferimenti normativi: G.U. n. 287 del 9 dicembre 2008 - Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali.

All'interno del SG-SI sono riportate le regole per lo smaltimento sicuro dei dispositivi elettrici ed elettronici contenenti dati personali consistenti sostanzialmente in una formattazione di basso livello dei dispositivi di memorizzazione.

## Registro dei trattamenti

### Nomi e dati di contatto

*Riferimenti normativi: GDPR, Art. 30 - Registri delle attività di trattamento.*

Il Titolare dei Trattamenti posti in essere sono l'Azienda e la Controllata nel loro complesso. La persona di contatto per il SG-GDPR e il SG-SI (Responsabile Privacy interno) è Ilario Gavioli, Legale Rappresentante di INTESYS S.r.l. (ilario.gavioli@intesys.it). Questo riferimento è valido anche per la Controllata.

Non esistono Contitolari dei Trattamenti.

La designazione di un Data Protection Officer è obbligatoria:

- se le attività principali del titolare del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
- se le attività principali del titolare del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Sulla base di una valutazione di impatto dei trattamenti effettuati sui diritti e sulle libertà degli interessati, vedi il paragrafo Analisi dei rischi Sicurezza e Privacy (DPRA), i trattamenti effettuati dall'Azienda e dalla Controllata:

- non richiedono il monitoraggio regolare e sistematico degli interessati;
- non consistono in un trattamento di dati su "larga scala", tenuto conto del numero di soggetti interessati dal trattamento, del volume e delle tipologie di dati, della durata e della portata geografica dell'attività di trattamento;
- non consistono in un trattamento di dati particolari o penali.

Mancando i requisiti richiesti dal Regolamento, il Titolare non ha ritenuto opportuno procedere alla nomina di un Data Protection Officer ne' per la Azienda ne' per la Controllata.

### Registri dei trattamenti

*Riferimenti normativi: GDPR, Art. 30 - Registri delle attività di trattamento. GDPR, Art. 44 - Principio generale per il trasferimento, GDPR, Art. 45 - Trasferimento sulla base di una decisione di adeguatezza, GDPR, Art. 46 - Trasferimento soggetto a garanzie adeguate, GDPR, Art. 47 - Norme vincolanti d'impresa, GDPR, Art. 48 - Trasferimento o comunicazione non autorizzati dal diritto dell'Unione, GDPR, Art. 49 - Deroghe in specifiche situazioni, GDPR, Art. 50 - Cooperazione internazionale per la protezione dei dati personali.*

Sono istituiti il Registro delle Attività di Trattamento di Titolarità di INTESYS S.r.l. e il Registro delle Attività di Trattamento di Titolarità di INTESYS Openway S.r.l., sviluppato in coerenza con l'Art. 30 del Regolamento. Tali documenti indicano le figure di responsabilità espressamente richieste dalla norma e riporta le seguenti informazioni:

- denominazione trattamento;
- descrizione trattamento;
- funzioni interessate;
- trattamento svolto in contitolarità;
- dati identificativi del contitolare;
- finalità del trattamento;
- categorie di interessati;
- categorie di dati trattati (es. comuni, particolari, genetici, biometrici, penali, ecc.);

- destinatari a cui vengono comunicati i dati (es. interni, esterni, ecc.) e modalità di trasmissione;
- attività di trattamento esternalizzate;
- termini temporali per la cancellazione dei dati personali oggetto di trattamento;
- localizzazione dei dati (es. database coinvolti nel trattamento, localizzazione fisica dei supporti di memorizzazione, localizzazione logica dei dati, applicazioni IT utilizzate, ecc.);
- condizioni di liceità (es. consenso dell'interessato, adempimento di un contratto, compito di interesse pubblico, ecc.);
- modalità di trattamento (es. raccolta, archiviazione, consultazione, modifica, organizzazione, ecc.);
- svolgimento di un Data Protection Impact Assessment sul trattamento considerato e motivazioni alla base della necessità di una valutazione d'impatto.

Per l'Azienda e per la Controllata è istituito inoltre il Registro delle Attività di Trattamento di Titolarità di Terzi (RAT-TTI/RAT-TTO), sviluppato in coerenza con l'Art. 30 del Regolamento. Tale documento indica le figure di responsabilità espressamente richieste dalla norma e riporta le seguenti informazioni:
- Dati identificativi del Titolare;
- Identificativo del trattamento e descrizione;
- Tipologie di trattamenti;
- Categorie di dati;
- Funzioni interessate;
- Localizzazione e utilizzo;
- Trasferimento all'estero;
- Misure di sicurezza adottate;

I registri dei trattamenti vengono revisionati sotto la responsabilità del Responsabile Privacy interno e con la collaborazione dei Responsabili delle Funzioni interessate:
- Con cadenza almeno annuale (entro il 31 marzo);
- In occasione di rilevanti variazioni dei trattamenti di dati personali;
- In occasione di rilevanti variazioni dell'organizzazione interna o delle norme vigenti in tema di protezione dei dati personali.

### Descrizione generale di misure tecniche e organizzative di sicurezza

*Riferimenti normativi: GDPR, Art. 30 - Registri delle attività di trattamento.*

Le misure organizzative e tecniche adottate dall'Azienda per assicurare la sicurezza delle informazioni e la protezione dei dati personali trattati, traggono ispirazione dalla linee guida UNI CEI ISO/IEC 27001 e dal regolamento UE 679/2016 (General Data Protection Regulation).

La sicurezza del patrimonio informativo viene realizzata garantendone:
- l'integrità: l'accuratezza, la completezza dei dati e dei relativi metodi di elaborazione;
- la riservatezza: la disponibilità dei dati è concessa solo ed esclusivamente ai soggetti che hanno autorizzazione ad accedervi;
- la disponibilità: gli utenti autorizzati possono accedere ai dati quando richiesto e ogni qual volta ciò sia necessario.

In particolare l'Azienda è consapevole che i dati personali oggetto di trattamento devono essere custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione e perdita anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'Azienda considera che la protezione del proprio sistema informativo permetta di:
- svolgere al meglio i propri compiti istituzionali;
- garantire la correttezza degli scambi informativi con i propri clienti e i propri fornitori;
- garantire la tutela della privacy in tutti gli ambiti di trattamento di dati personali, secondo quanto previsto dalla normativa vigente.

All'interno di SG-SI e SG-GDPR vengono raccolte le norme e le modalità operative che tutti i dipendenti dell'azienda devono rispettare al fine di garantire la sicurezza del patrimonio informativo aziendale e al fine di ottemperare gli obblighi di legge in materia di trattamento di dati personali.

## Governance del sistema

### Modello organizzativo Privacy

*Riferimenti normativi: GDPR, Art. 24 - Responsabilità del titolare del trattamento; GDPR, Art. 26 - Contitolari del trattamento; GDPR, Art. 27 - Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione; GDPR, Art. 28 - Responsabile del trattamento; GDPR, Art. 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento; GDPR, Art. 37 - Designazione del responsabile della protezione dei dati; GDPR, Art. 38 - Posizione del responsabile della protezione dei dati; GDPR, Art. 39 - Compiti del responsabile della protezione dei dati.*

Le figure di responsabilità previste e nominate secondo le direttive del Regolamento (UE) 679/2016 in materia di tutela dei dati personali e comunque implicate in attività relative alla sicurezza sono le seguenti:
- Titolare del Trattamento, nella persona del Legale Rappresentante della Azienda e della Controllata;
- Responsabile Privacy Interno (RPI), unico per la Azienda e per la Controllata, coincidente con il ruolo di Responsabile per la Sicurezza per quanto riguarda SG-SI unico per la Azienda e per la Controllata, nella persona di Ilario Gavioli;
- Responsabile Interno per i Trattamenti, nella persona del RPI;
- Responsabili Esterni per i Trattamenti , nella persona del RPI;
- Incaricati per il trattamento, tutti i dipendenti e collaboratori della Azienda e della Controllata secondo quanto stabilito in SG-SI.
- Amministratori di Sistema, di Rete e di Database, secondo i documenti di nomina previsti.
- Responsabile IT della Azienda e della Controllata, nella persona di Romano Rosponi
- Responsabile della Sicurezza Fisica della Azienda e della Controllata, nella persona di Alberto Gaiga

***ATTENZIONE: All'interno dei due Manuali SI-GDPR e SG-SI in alcuni casi può essere utilizzato il termine Responsabile della Sicurezza per intendere Responsabile Privacy Interno in quanto il ruolo è unico.***

Come descritto all'interno del "Paragrafo 3.1 - Nomi e dati di contatto", mancando i requisiti richiesti dal Regolamento, il Titolare non ha ritenuto opportuno procedere alla nomina di un Data Protection Officer.

**Responsabili Interni per il Trattamento**

*Riferimenti normativi: vedi 3.1 - Modello organizzativo Privacy*

Il Titolare della Azienda e della Controllata procede alla nomina di un unico Responsabile Interno per il Trattamento (RIT) indicando chiaramente gli ambiti di operatività e le responsabilità per la protezione dei dati personali, quali:

- deve fornire supporto al Titolare nello svolgimento degli adempimenti richiesti dal Regolamento (UE) 679/2016 in materia di protezione dei dati personali, inclusa la compilazione e l'aggiornamento del Registro dei Trattamenti;
- deve rispettare degli obblighi di sicurezza;
- deve notificare tempestivamente le violazioni di dati personali al Garante della Privacy e se del caso, agli interessati;
- deve effettuare la protezione dei dati personali fin dalla progettazione;
- deve procedere alla nomina degli incaricati e degli amministratori di sistema;
- in presenza di nuovi trattamenti, deve predisporre l'invio dell'informativa agli interessati, l'ottenimento del relativo consenso e garantire agli interessati l'effettivo esercizio dei diritti;
- deve verificare, per quanto di competenza e relativamente al regolamento UE 679/2016, che siano adottate le misure di sicurezza tecniche e organizzative adeguate al rischio e stabilite dall'azienda;
- deve informare il Titolare in merito a qualsiasi fatto che possa avere dei riflessi o delle conseguenze sull'attività o sulle responsabilità del Titolare stesso;

**Incaricati per il Trattamento**

Il Titolare della Azienda e della Controllata procede alla nomina degli Incaricati per il Trattamento (IT) indicando chiaramente gli ambiti di operatività e le responsabilità per la protezione dei dati personali, quali:

- trattare i dati in modo lecito e secondo correttezza;
- effettuare le sole operazioni di trattamento necessarie allo svolgimento della propria mansione nel rispetto del Regolamento (UE) 679/2016 in materia di protezione dei dati personali;
- attenersi alle istruzioni impartite dal Titolare o dal Responsabile;
- adottare le misure di sicurezza stabilite dall'azienda così da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali;
- prevenire e/o evitare la comunicazione o diffusione illecita dei dati;
- informare tempestivamente il Responsabile in merito a ogni questione rilevante ai sensi del Regolamento (UE) 679/2016 in materia di protezione dei dati personali;
- astenersi dall'adozione di autonome decisioni in merito alle finalità e alle modalità del trattamento.

**Responsabili Esterni per il Trattamento**

*Riferimenti normativi: vedi 3.1 - Modello organizzativo Privacy*

Il Titolare della Azienda e della Controllata procede alla nomina dei Responsabili Esterni per il Trattamento (RET) nella persona del RPI indicando chiaramente gli ambiti di operatività e le responsabilità per la protezione dei dati personali quali:

- trattare i dati seguendo le modalità di trattamento concordate con il Titolare;
- garanzia che i soggetti incaricati dal Responsabile Esterno siano informati e tenuti al rispetto della privacy;
- localizzazione dei dati personali trattati;
- doveri relativi a cancellazione, rettifica e portabilità dei dati;
- tempi di conservazione;
- divieto di ricorso a subappalti senza autorizzazione del Titolare dei Trattamenti;
- obblighi di comunicazione in caso di violazioni di sicurezza in tempi predefiniti;
- eventuale trasferimento dei dati in paesi UE/extra UE o organizzazioni internazionali con indicazione delle relative garanzie;
- diritto di svolgere audit da parte del Titolare del Trattamenti;
- presenza di procedure relative ai diritti dell'interessato;
- presenza di procedure relative alla "Data Breach Notification" nei confronti del Titolare dei Trattamenti con indicazione del tempo di segnalazione dopo la rilevazione della violazione;
- norme generali per l'applicazione dei principi di "Privacy by Design" e "Privacy by Default".

**Nomina a Responsabile Esterno per il Trattamento**

Nell'ambito dei trattamenti di dati personali effettuati dalla Azienda e dalla Controllata rientrano anche quelli eventualmente affidati all'azienda da specifici Clienti.

In conformità con l'Art. 28 del Regolamento, l'Azienda e la Controllata presentano adeguate garanzie di sicurezza e adotta misure tecniche e organizzative idonee a garantire che i trattamenti effettuati soddisfino i requisiti del Regolamento, a garanzia della tutela dei diritti dell'interessato.

Le attività di trattamento che l'Azienda e la Controllata effettuano, per conto di specifici Clienti, sono puntualmente elencate e descritte nei rispettivi registri dei trattamenti.

**Nomine, informative, consensi, nomine e clausole contrattuali**

*Riferimenti normativi: GDPR, Art. 7 - Condizioni per il consenso; GDPR, Art. 8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione; GDPR, Art. 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato; GDPR, Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; GDPR, Art. 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.*

Le nomine a Responsabile Interno per il Trattamento, Incaricato per il Trattamento, Responsabile Esterno per il Trattamento, Sub Responsabile Esterno per il Trattamento avvengono, per la Azienda e per la Controllata, in forma di lettera controfirmata e copia di tale documentazione è disponibile in cartaceo presso la segreteria amministrativa.

Il RPI (anche Responsabile Sicurezza SG-SI) verifica e aggiorna le nomine in questione ogniqualvolta sia necessario, in virtù di variazioni dell'organizzazione o delle attività di trattamento svolte. Tali aggiornamenti sono svolti al fine di garantire che vi sia corrispondenza tra i documenti di nomina (ovvero le autorizzazioni a svolgere specifiche attività di trattamento) e trattamenti effettuati.

Sono previste specifiche informative per assicurare la trasparenza dei trattamenti effettuati e la corretta informazione dei soggetti interessati. In particolare:
- Informative per i dipendenti e collaboratori;
- Informative relative a richieste di lavoro e relativa trasmissione di dati personali e CV;
- Informativa su raccolta dati digitale sul sito Web aziendale;
- Informativa relativa alla videosorveglianza.

È responsabilità del RPI organizzare le procedure in modo che le informative siano fatte chiaramente conoscere all'interessato al momento della raccolta dei dati.

Le informative contengono le seguenti informazioni minime:
- identità e dati di contatto del Titolare dei Trattamenti e del suo rappresentante;
- finalità del trattamento e condizioni di liceità dello stesso;
- legittimi interessi perseguiti dal Titolare dei Trattamenti;
- destinatari dei dati personali;
- termini di cancellazione dei dati personali o criteri per la determinazione di tale periodo;
- diritti dell'interessato;
- fonte da cui hanno origine i dati personali;
- conseguenze sull'interessato derivanti da un eventuale, se possibile, mancato consenso;
- esplicitazione della effettuazione di un processo decisionale automatizzato (es. profilazione).

L'eventuale consenso dell'interessato deve essere raccolto solo dopo aver consegnato all'interessato stesso l'informativa. In particolare:
- il consenso viene espresso oralmente per il trattamento dei dati personali comuni;
- il consenso viene espresso mediante dichiarazione scritta, anche attraverso mezzi elettronici e deve essere chiaramente ed esplicitamente documentato per il trattamento dei dati particolari e penali;
- il consenso non è richiesto per i trattamenti svolti sulla base di specifiche condizioni di liceità indicate dal Regolamento (UE) 679/2016 in materia di protezione dei dati personali, ovvero:
  - adempimento di un obbligo di legge al quale è soggetto il Titolare;
  - compito di interesse pubblico o di pubblici poteri di cui è investito il Titolare;
  - perseguimento di legittimo interesse del titolare o di terzi (a condizione che non coinvolga un minore o che non vengano utilizzate nuove tecnologie);
  - salvaguardia degli interessi vitali dell'interessato o di terzi;
  - svolgimento di un contratto di cui è parte l'interessato;
  - esecuzione di misure precontrattuali richieste dall'interessato.

È responsabilità del RPI assicurare una corretta gestione e conservazione delle informative fornite agli interessati e dei relativi consensi, al fine di:
- garantire che le attività di trattamento dei dati personali siano svolte nel pieno rispetto delle condizioni di liceità poste dal Regolamento;
- assicurare la possibilità di ricostruire, quando necessario:
  - l'elenco degli interessati ai quali è stata trasmessa un'informativa, in quale versione ed in quale data;
  - la data in cui è stato firmato il consenso e il tipo di consenso ricevuto, ovvero le scelte espresse dall'interessato nel caso di molteplici trattamenti che richiedono il consenso.

È dunque di importanza fondamentale che la Azienda e la Controllata registrno ed archivino le informative e i consensi raccolti in modo da poterli facilmente recuperare in caso di necessità, verifica o contestazione.

### Data Protection Impact Assessment (DPIA)

*Riferimenti normativi: GDPR, Artt. 35 - Valutazione d'impatto sulla protezione dei dati; GDPR, Art. 36 - Consultazione preventiva.*

Prima di effettuare trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Regolamento richiede lo svolgimento di una valutazione d'impatto del trattamento sui diritti e sulle libertà dell'interessato (Data Protection Impact Assessment o DPIA), i cui risultati devono essere adeguatamente formalizzati. LA DPIA è richiesta, in particolare, nei casi seguenti:
- valutazione sistematica di aspetti personali, basata su un trattamento automatizzato sulla quale si fondano decisioni con effetti giuridici sugli interessati;
- trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati di cui all'articolo;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Premesso che un singolo DPIA può esaminare un insieme di trattamenti simili che presentano rischi analoghi, l'istruttoria per la valutazione d'impatto deve essere effettuata:
- Identificando le possibili minacce alla sicurezza dei trattamenti;
- Considerando i requisiti di riservatezza, disponibilità e integrità dei dati personali;
- Considerando le necessarie misure di protezione tecnico-organizzativa da attuare per rendere il rischio accettabile.

Nel caso le misure ipotizzate siano ritenute adeguate (ovvero idonee a abbassare il livello di rischio fino a renderlo accettabile) il trattamento può essere attivato. In caso contrario, il trattamento non può essere attivato senza l'autorizzazione preventiva del Garante della Privacy.

Sulla base dei risultati della "Analisi dei rischi Sicurezza e Privacy (DPRA)" (vedi paragrafi successivi) ed in seguito ad una approfondita valutazione, si rileva che i Trattamenti attualmente posti in essere dalla Azienda e dalla Controllata (raccolti all'interno del Registro dei Trattamenti) riguardano dati personali comuni e non presentano rischio elevato per i diritti e le libertà delle persone fisiche. Di conseguenza, non devono essere sottoposti a Data Protection Impact Assessment.

### Data Protection by Design e by Default

*Riferimenti normativi: GDPR, Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*

La Azienda e la Controllata sviluppano e adottano metodologie e procedure per applicare i principi di "Privacy by Design" e "Privacy by Default" a tutte le attività di trattamento che coinvolgono dati personali. Le misure tecniche e organizzative adottate dall'azienda per questo scopo hanno come obiettivo la definizione di trattamenti di dati personali solo per finalità legittime e chiaramente determinate e con i dati personali minimi necessari ad ogni specifica finalità di trattamento.

Il Titolare del Trattamento deve identificare, fin dalla progettazione dei nuovi trattamenti relativi ai dati personali, delle misure tecniche e organizzative idonee a garantire il rispetto dei Principi Privacy.

Le soluzioni tecniche e organizzative adottate dall'Azienda e dalla Controllata devono garantire che siano trattati "per impostazione predefinita" (Privacy by Default), solo ed esclusivamente i dati personali necessari per il raggiungimento delle finalità di trattamento dichiarate. Tale obbligo vale in termini di:

- quantità di dati personali raccolti;
- portata del trattamento;
- periodo di conservazione;
- accessibilità dei dati personali.

La definizione delle misure idonee avviene per differenza rispetto ad una serie di misure per la sicurezza dell'informazione previste nel SG-SI. All'interno del Registro dei Trattamenti la scheda dedicata al singolo trattamento riporta eventuali misure di sicurezza aggiuntive rispetto al default.

Per essere conforme al Regolamento, il Titolare del Trattamento deve assicurare che le soluzioni tecnico-organizzative definite in fase di progettazione siano:

- correttamente implementate in fase di realizzazione e collaudate prima della loro adozione;
- oggetto di validazione in caso di cambiamenti tecnico-organizzativi che interessano i processi di trattamento di dati personali;
- migliorabili nel tempo in relazione alla evoluzione delle tecnologie.

Nel caso di Trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, la procedura prevede e mette in atto regole di "Project Management" e di "Change Management".

Per quanto riguarda il "Project Management", l'attivazione di nuovi trattamenti relativi a dati personali "particolari e penali" deve prevedere un processo progettuale organizzato per fasi (raccolta dei requisiti e studio di fattibilità, progettazione del trattamento, analisi del rischio e valutazione degli impatti sui diritti e sulle libertà dell'interessato, sviluppo e realizzazione del progetto, test e collaudo, validazione e messa in produzione), correttamente impostato, controllato e posto in essere con il coinvolgimento di tutte le funzioni aziendali interessate.

Per quanto riguarda il "Change Management", eventuali cambiamenti che modifichino i processi aziendali, le tecnologie utilizzate o le misure tecniche/organizzative per la protezione dei dati personali devono essere verificati (prima dell'applicazione) e autorizzati dal Titolare del Trattamento.

Ulteriori dettagli operativi e procedurali sono approfonditamente trattati e descritti nel documento SI-GDPR Linee guida privacy by design e by default accessibile online nella Wiki aziendale.

## Diritti e richieste degli interessati

*Riferimenti normativi: GDPR, Art. 15 - Diritto di accesso dell'interessato; GDPR, Art. 16 - Diritto di rettifica; GDPR, Art. 17 - Diritto alla cancellazione (diritto all'oblio); GDPR, Art. 18 - Diritto di limitazione di trattamento; GDPR, Art. 19 - Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento; GDPR, Art. 20 - Diritto alla portabilità dei dati; GDPR, Art. 21 - Diritto di opposizione; GDPR, Art. 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.*

L'Azienda ha sviluppato una procedura per la gestione dei diritti dell'interessato e per l'adempimento a eventuali richieste entro i termini previsti dal GDPR. La procedura, estesa alla Controllata, prevede, per ogni trattamento posto in essere e all'interno della scheda descrittiva delle caratteristiche del trattamento, l'insieme delle operazioni da mettere in campo per garantire all'interessato i propri diritti, in particolare:

- Con riferimento al diritto di accesso di dati personali: una procedura per garantire all'interessato di esercitare il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso e di ottenere l'accesso a tali dati.
- Con riferimento al diritto di rettifica e cancellazione dei dati personali: una procedura che assicura, senza ingiustificato ritardo, il diritto dell'interessato di ottenere la rettifica e/o la cancellazione dei dati personali che lo riguardano, ottenendo la revoca del consenso su cui si basa il trattamento se non sussistono motivi legittimo prevalente per procedere al trattamento stesso. La procedura garantisce anche:
  - il controllo sulla effettiva scadenza dei termini del trattamento;
  - la presenza di procedure di cancellazione dei dati trattati tramite sistemi IT (es. database, back-up, disaster recovery, dispositivi mobili, ecc.);
  - la presenza di procedure di cancellazione dei dati non trattati tramite sistemi IT (es. cancellazione di documentazione cartacea);

    - la registrazione delle cancellazioni effettuate e dei relativi controlli.
- Con riferimento al diritto di limitazione del trattamento: la procedura assicura l'esercizio del diritto dell'interessato alla limitazione del trattamento quando è in dubbio l'esattezza dei dati personali (per il periodo necessario al titolare del trattamento per verificarne l'esattezza), il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati e chiede invece che ne sia limitato l'utilizzo, l'interessato si oppone al trattamento in attesa della verifica sull'eventuale prevalenza dei motivi legittimi del Titolare.
- Con riferimento al diritto di portabilità dei dati: la procedura assicura l'esercizio del diritto dell'interessato di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, di trasmettere i dati a un altro titolare senza impedimenti e/o ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
- Con riferimento al diritto di opposizione: la procedura assicura l'esercizio del diritto dell'interessato a opporsi, in qualsiasi momento, al trattamento dei dati personali che lo riguardano.
- Con riferimento al diritto a non essere soggetto ad attività di profilazione: la procedura assicura l'esercizio del diritto dell'interessato, in caso di esplicita richiesta e di modifica del profilo di consenso, di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che lo riguardano.

In ogni caso le procedure di gestione dei diritti dell'interessato prevedono:
- una valutazione della "liceità" della richiesta;
- in caso di richiesta "non lecita" la comunicazione del rifiuto;
- in caso di richiesta "lecita" la comunicazione dell'accettazione;
- le modalità di esercizio dei diritti dei soggetti interessati.

Ulteriori dettagli operativi e procedurali sono approfonditamente trattati e descritti nel documento SI-GDPR Linee guida diritti interessato accessibile online nella Wiki aziendale.

## Protezione dei dati: rischi e misure di sicurezza

### Analisi dei rischi Sicurezza e Privacy (DPRA)

*Riferimenti normativi: GDPR, Art. 32 - Sicurezza del trattamento.*

Periodicamente vengono svolte istruttorie sistematiche di Risk Assessment aventi come oggetto i dati personali e le attività di trattamento degli stessi posti in essere dall'Azienda e dalla Controllata.

Tali istruttorie di Risk Assessment sono finalizzate:
- alla definizione di criteri univoci per la valutazione del rischio relativo alla sicurezza delle informazioni e alla protezione dei dati personali;
- all'identificazione dei rischi che possono avere un impatto sul patrimonio informativo aziendale o sui diritti e sulle libertà dei soggetti interessati dalle attività di trattamento (Risk Identification);
- all'analisi della natura dei rischi individuati, attraverso l'identificazione delle minacce che li possono generare, finalizzata all'identificazione del livello di rischio a cui l'Azienda è esposta (Risk Analysis);
- alla comparazione dei risultati derivanti dall'attività di Risk Analysis con i criteri di definiti, in modo da determinare se i rischi analizzati sono accettabili o meno da parte dell'Azienda (Risk Evaluation);
- all'individuazione delle misure di sicurezza, organizzative e tecniche, idonee a mitigare i rischi oggetto di analisi (Risk Treatment).

Ai fini di valutare il correttamente il rischio relativo alla sicurezza delle informazioni e alla protezione dei dati personali, l'analisi dei rischi fa riferimento ai seguenti standard internazionali:
- ISO 27001 - Information security management systems requirements;
- ISO 27002 - Code of practice for information security controls;
- ISO 27005 - Information security risk management;
- ISO 29151 - Code of practice for personally identifiable information protection;
- ISO 31000 – Risk management principles and guidelines.

Il rischio viene calcolato mediante i parametri di probabilità, impatto e vulnerabilità. La determinazione dei valori di questi parametri è effettuata dai Responsabili delle aree aziendali interessate che procedono a esaminare i controlli di sicurezza previsti dagli Standard Internazionali ISO 27001:2013 e ISO 29151:2017 assegnando valori di vulnerabilità che rappresentano il livello di applicazione dei controlli nell'area considerata. La "Tabella di Risk Assessment" (TRA) che se ne ricava definisce il quadro generale dei rischi per la sicurezza delle informazioni e dei dati personali a cui l'Azienda è esposta.

Tutti i dettagli della Analisi dei Rischi sono descritti nella pagina
Gestione del Rischio
che contiene il particolare documento
**DATA PROTECTION RISK ASSESSMENT**
da considerare parte integrante del presente SG-GDPR.

## Violazioni dati personali

### Criteri per valutare se effettuare una notifica di violazione dei dati personali trattati

*Riferimenti normativi: GDPR, Artt. 33 - Notifica di una violazione dei dati personali all'autorità di controllo; GDPR, Art. 34 - Comunicazione di una violazione dei dati personali all'interessato.*

l'Azienda ha adottato un sistema di Incident Management e un sistema di Analisi dei Rischi per la sicurezza delle informazioni e dei dati personali volti a formalizzare, approvare e diffondere regole e procedure per l'individuazione, la valutazione, la classificazione e la successiva gestione:
- degli incidenti, intesi come eventi di sicurezza delle informazioni in grado di arrecare danno al patrimonio informativo aziendale o ledere i diritti e le libertà degli interessati;

- delle vulnerabilità organizzative o tecnologiche che potrebbero essere sfruttate da minacce in grado arrecare danno al patrimonio informativo aziendale o ledere i diritti e le libertà degli interessati.

Tali regole e procedure permettono l'identificazione e la corretta gestione degli eventi di sicurezza che riguardano dati personali e che, per la loro gravità (ovvero per il loro impatto sui diritti e sulle libertà degli interessati) necessitano di notifica al Garante della Privacy o ai soggetti interessati, nei modi e nei tempi previsti dalla legge.

Tutte le regole e procedure del presente paragrafo sono estese anche alla Controllata.

### Processo per la notifica di violazioni di dati personali

*Riferimenti normativi: vedi 5.1 - Criteri per valutare se effettuare o meno una notifica di violazione di dati personali.*

L'Azienda e la sua Controllata ha adottato, formalizzato e diffuso linee guida per la notifica delle violazioni di dati personali (al Garante della Privacy ed eventualmente, ai soggetti interessati) nei modi e nei tempi previsti dalla legge.

Tali regole specificano l'impegno del Titolare a notificare al Garante della Privacy eventuali violazioni dei dati personali di cui si venga a conoscenza, ad eccezione dei casi in cui il Titolare sia in grado di dimostrare che la violazione non comporti in alcun modo rischi per i diritti e le libertà degli interessati (es. dati oggetto di violazione protetti da crittografia).

Nel caso in cui i rischi derivanti da una violazione siano considerati “elevati” dal Titolare o dal Garante della Privacy, la notifica è rivolta anche ai soggetti interessati, a meno che siano state applicate misure di sicurezza atte a rendere intellegibili i dati nel momento in cui sono violati (es. dati oggetto di violazione protetti da crittografia).

La notifica della violazione contiene le seguenti informazioni:
- data di comunicazione della violazione;
- nome del referente aziendale (Data Protection Officer o altra figura designata dal Titolare);
- natura e descrizione della violazione dei dati;
- data e ora in cui la violazione si è verificata;
- data e ora in cui la violazione è stata rilevata;
- luogo in cui si è verificata la violazione;
- dispositivi oggetto della violazione;
- descrizione e ubicazione dei sistemi di elaborazione coinvolti;
- tipologie e numero stimato di soggetti interessati coinvolti;
- tipologia e numero stimato di dati personali oggetto della violazione;
- probabili conseguenze della violazione sui dati personali;
- misure tecniche e organizzative adottate (o che il Titolare intende adottare, come azione di rimedio, per evitare nuove violazioni);
- comunicazione della violazione ai soggetti Interessati (ed eventualmente, motivazione della “non-comunicazione”, se questa non è effettuata);
- contenuto della comunicazione agli interessati e canale utilizzato;
- altri soggetti coinvolti;
- altri Paesi coinvolti;

Ulteriori dettagli operativi e procedurali sono approfonditamente trattati e descritti nel documento Gestione violazioni di dati personali accessibile online nella Wiki aziendale nonchè gestiti operativamente da una applicazione software di Incident Management.

## Formazione, miglioramento ed audit

### Formazione

*Riferimenti normativi: GDPR, Art. 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.*

Come previsto nel SG-SI, tutto il personale implicato o nel trattamento dei dati o nella attuazione e controllo delle misure di sicurezza della Azienda e della Controllata viene coinvolto in un piano di formazione che prevede:
- informazioni su normativa vigente, sicurezza delle informazioni e protezione dei dati personali;
- criteri generali di sicurezza;
- modalità di utilizzo di user ID e parola chiave;
- modalità operative nelle sessioni telematiche di trattamento dati.

Le modalità prevedono la messa a disposizione di documenti e materiale didattico sulla Intranet aziendale e qualora ritenuto necessario, lo svolgimento di interventi formativi in aula.

Il personale coinvolto è tenuto a firmare, anche elettronicamente, una dichiarazione annuale di presa visione del materiale didattico.

Per i neo-assunti questa dichiarazione è richiesta tra gli obblighi contestuali all'inserimento lavorativo.

Nel caso di attività formative in aula verrà compilato e conservato un registro delle presenze.

Periodicamente verranno somministrati al personale coinvolto dei questionari a risposta multipla per testare l'effettivo apprendimento dei contenuti trasmessi.

Le attività di formazione, informazione, sensibilizzazione e addestramento saranno indirizzate a:
- i neoassunti;
- il personale che ha subito (o che subirà) un cambio di mansione;
- il personale coinvolto in cambiamenti organizzativi (es. modifica di processi, adozione di nuovi sistemi IT o tecnologie, ecc.);
- in generale, tutto il personale coinvolto nelle attività di trattamento di dati personali poste in essere dall'azienda.

### Verifiche periodiche e Piano di Miglioramento

*Riferimenti normativi: GDPR, Art. 32 - Sicurezza del trattamento, GDPR, Artt. 35 - Valutazione d'impatto sulla protezione dei dati.*

Il SG-GDPR viene revisionato ad intervalli regolari e comunque almeno una volta all'anno entro il 31 marzo, per garantirne l'effettiva attuazione e verificarne la reale adeguatezza.

Le attività di verifica dei processi e di adeguamento della documentazione di sistema prevede lo svolgimento di verifiche ispettive (Audit).

Gli Audit sono finalizzati a garantire la conformità al Regolamento delle Funzioni interne e dei Fornitori, i quali devono dimostrare il rispetto delle norme aziendali interne e delle clausole contrattuali in tema di protezione dati personali.

Lo svolgimento degli Audit, che avviene con cadenza almeno annuale, richiede le seguenti attività:

- definizione del programma di Audit: le visite ispettive devono essere pianificate precisando le aree di verifica, i trattamenti interessati (interni o affidati a Fornitori), le persone coinvolte (da avvisare con congruo anticipo), la data e la durata stimata dell'intervista. Il programma di Audit deve essere approvato dal Titolare del Trattamento;
- definizione delle check list di controllo: le checklist di controllo, da utilizzare nello svolgimento delle visite ispettive, devono essere predisposte in coerenza con gli obiettivi e l'ambito della verifica, considerando gli adempimenti del Regolamento che devono essere realizzati a cura del Titolare del Trattamento e dei Responsabili del Trattamento.
- svolgimento delle visite ispettive: dopo aver informato i presenti sugli obiettivi e sull'ambito della verifica ispettiva, il Responsabile dell'Audit coordina lo svolgimenti di opportune analisi relative alle soluzioni tecniche, organizzative e documentali oggetto della verifica (seguendo le check list di controllo preventivamente predisposta), registra i rilievi emersi durante le interviste (evidenze, osservazioni e non conformità) e organizza una riunione conclusiva nella quale sono comunicate ai partecipanti le risultanze della verifica ispettiva;
- verbale dei risultati delle visite ispettive: Il Responsabile dell'Audit redige un apposito verbale, che è successivamente consegnato al Titolare del Trattamento e ai Responsabili del Trattamento interessati, ponendo in evidenza eventuali non conformità che potrebbero comportare sanzioni a carico dell'Azienda (es. non conformità rispetto alla normativa vigente, misure di sicurezza inefficaci o mancanti, ecc.);
- pianificazione delle azioni correttive: il Titolare del Trattamento, d'intesa con il Responsabile della Sicurezza, assicura la redazione e l'attuazione di un piano di trattamento del rischio a fronte delle risultanze delle visite ispettive dando priorità alla soluzione delle "non conformità" più gravi, assegnando precise responsabilità e definendo i tempi attesi per la realizzazione del piano stesso.

La rilevazione costante delle non conformità permette di migliorare l'organizzazione per soddisfare le misure adottate, di introdurre nuove misure o modificare le esistenti permettendo un miglioramento continuo e costante del sistema nel suo complesso. Sono previste, da parte di terze parti, attività di audit per il piano interno e per l'attuazione delle norme da parte di responsabili esterni per il trattamento nominati da Intesys.

A cura del responsabile per la sicurezza viene redatto e aggiornato su base semestrale un documento che riporta attività interne di controllo e verifica delle procedure in essere con i relativi risultati ed eventuali azioni di miglioramento programmate.

Tutte le regole e procedure del presente paragrafo sono estese anche alla Controllata.