Modello organizzativo per la protezione dei dati e per la sicurezza delle informazioni

SVILUPPO INVESTIMENTI TERRITORIO S.R.L.

Identificativo nazionale (C.F.): 09969560011

Stato delle revisioni

Anno	Data	Descrizione
2021	09/03/2021	revisione generale dei regolamenti e delle politiche di protezione dei dati; prima emissione del sistema; aggiornamento dei riferimenti normativi, delle procedure e dei modelli dei documenti di attuazione

Luogo, Data

Firma

DE MARCHI MONICA

Pagina intenzionalmente vuota

Sommario

1 Campo di applicazione

Il Modello organizzativo per la protezione dei dati personali, indicato anche come Sistema, definisce le politiche e gli standard di protezione e sicurezza in merito al trattamento dei dati e delle informazioni.

Il sistema copre il trattamento di tutti i dati personali, compresi quelli sensibili, giudiziari e particolari.

Gli adempimenti, misure e ruoli sono tratti dalle norme per la protezione dei dati personali

Le informazioni da difendere possono presentarsi in varie forme: su carta, in formato elettronico, trasmesse per posta elettronica, scambiate a voce durante conversazioni, su filmati. In qualunque forma o mezzo in cui vengono trattate le informazioni, esse devono sempre essere adeguatamente protette. Dunque, il sistema si applica al trattamento di tutti i dati e informazioni per mezzo di:

1. Strumenti elettronici di elaborazione (campo digitale)
2. Strumenti non elettronici, come supporti cartacei (campo analogico)

Il sistema deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione di SVILUPPO INVESTIMENTI TERRITORIO S.R.L., ciascuno per quanto di propria competenza e spettanza. Quindi, tutti i soggetti (incaricati e non) che operano nell'ambito dell'organizzazione di SVILUPPO INVESTIMENTI TERRITORIO S.R.L., compresi i dipendenti, i collaboratori non dipendenti, i consulenti esterni, gli addetti alle manutenzioni che per effetto della loro attività possono avere accesso ai dati, gli ospiti e tutti coloro che accedano all'interno delle sedi e dei locali nella disponibilità giuridica di SVILUPPO INVESTIMENTI TERRITORIO S.R.L., ed utilizzino le strutture messe a disposizione sono tenuti al rispetto scrupoloso del Sistema, nell'ambito delle proprie attività.

L'inosservanza delle norme stabilite nel Sistema è suscettibile di provvedimenti, anche sanzionatori, commisurati alla gravità della violazione.

2 Riferimenti normativi

Norme cogenti applicabili:

- Regolamento (UE) n. 2016/679 - GDPR
- Norma nazionale – D.Lgs. 196/2003 integrato con le modifiche introdotte dal D.Lgs. 101/2018

Norme tecniche di riferimento

- ISO 31000 “Risk Management”
- ISO IEC 27001:2016 “Sistema di Gestione della Sicurezza delle Informazioni”
- ISO IEC 29100:2011 “Privacy Framework”

3 Struttura del Modello organizzativo

SVILUPPO INVESTIMENTI TERRITORIO S.R.L. adotta il principio funzionale integrato da una concezione fondata su un'ottica organizzativa per processi secondo una visione sistemica. Tutti i processi aventi influenza sulla protezione dei dati personali sono governati da documenti specifici che definiscono modalità operative e responsabilità nell'ambito del processo descritto.

La documentazione del Sistema include procedure, documenti e registrazioni. Il grado di estensione e la natura della documentazione sono stati concepiti tuttavia anche per rispondere alla natura e prassi organizzativa interna e in ragione della complessità e dell'interazione tra i processi, della competenza e professionalità del personale e della dimensione e del tipo di organizzazione.

La **Politica** è la dichiarazione sistemica che definisce formalmente verso tutti i portatori di interessi gli indirizzi generali in materia di protezione dei dati personali. Legati alla politica e ad essa coerenti, gli Obiettivi sono espressi a livello settoriale (per funzione / linea di servizio / processo / ecc.) in forma misurabile.

Il **Mansionario** dei ruoli, funzioni, poteri e compiti specifica gli incarichi, le responsabilità operative e le autorità necessarie per il funzionamento del sistema.

Le **Procedure** sono documenti, generalmente di carattere interfunzionale, che disciplinano e coordinano le attività, definiscono modalità operative, risorse, responsabilità al fine di garantire il perseguimento della politica e degli obiettivi all'interno dei processi.

Inoltre SVILUPPO INVESTIMENTI TERRITORIO S.R.L. per il personale interno, garantisce l'acquisizione e la diffusione di documenti di origine esterna quali, per es.: Leggi, Norme, Bandi, Direttive, Disposizioni di Dettagli, Verbali di controllo, ecc..

I **Documenti di Registrazione** sono modelli necessari per eseguire in modo corretto e oggettivo attività regolamentate da Procedure/Istruzioni/Disposizioni, ecc.. Le registrazioni richieste sono predisposte in forma cartacea o elettronica e vengono conservate per fornire evidenza della conformità ai requisiti e dell'efficace funzionamento del sistema di gestione. Al fine di garantire nel tempo le necessarie informazioni circa la corretta attuazione dei processi e dei servizi formativi ed orientativi, documenti cartacei ed elettronici relativi a: progetti, attività, percorsi, ecc. sono gestiti nel rispetto dell'identificazione e della rintracciabilità di pratiche e documenti. Più precisamente a conclusione di ogni procedura e istruzione di lavoro sono individuati i criteri, le responsabilità e le modalità di gestione dei documenti prodotti.

4 Politica adottata

In generale, la gestione dei dati e delle informazioni deve essere ed è improntata a soddisfare i regolamenti e requisiti cogenti definiti dalle Autorità Pubbliche; in particolare, il trattamento dei dati personali procede nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il Sistema deve permettere di comprovare («principio di responsabilizzazione» ai sensi del Reg.§5.2) il rispetto dei principi applicabili al trattamento di dati personali.

Inoltre, devono essere e sono rispettati i requisiti contrattuali e di sicurezza stabiliti dalle controparti interessate.

5 Obiettivi del sistema

Lo scopo del sistema è quello di proteggere le informazioni da una ampia serie di minacce, previa conformità agli obblighi normativi, allo scopo di garantire il regolare svolgimento delle attività di SVILUPPO INVESTIMENTI TERRITORIO S.R.L., minimizzando gli eventuali danni che possono essere economici e relativi alla immagine, massimizzando il ritorno sugli investimenti eseguiti.

Gli obiettivi perseguiti per la sicurezza delle informazioni sono

- riservatezza (controllo di accesso ai file memorizzati o scambiati)
- integrità (preservazione del contenuto in base alla versione)
- disponibilità (utilizzabilità quando necessario)

La non ripudiabilità dei documenti non è ritenuta al momento essenziale, salvo per i documenti con valore legale.

La realizzazione di questi obiettivi è una sfida sia di natura tecnica, sia di natura organizzativa, da cui l'esigenza di diffondere e applicare il sistema a tutti i livelli.

Le misure di tipo di organizzativo consistono in procedure e regolamenti atti ad ottenere un livello di sicurezza e protezione delle informazioni coerente con gli obiettivi e le strategie di SVILUPPO INVESTIMENTI TERRITORIO S.R.L.. Quelle di tipo fisico, consistono nell'impiego di mezzi ed infrastrutture: ad esempio, per prevenire l'accesso a personale non autorizzato o per garantire la continuità delle attività prevenendo interruzioni dovute a cause esterne ed eventi ambientali. Quelle di tipo logico, consistono in misure tecnologiche: ad esempio per prevenire la possibilità di accesso alle risorse informatiche da parte di programmi software o personale non autorizzato o per rilevare gli accessi e le attività relative a violazioni e tentativi di intrusione delle informazioni.

6 Definizioni

Si richiamano le definizioni presenti nei riferimenti normativi e, in particolare, riportando, integrando e coordinando i lemmi richiamati, si definiscono per comodità:

“dato personale”, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

“dati particolari”, dati personali che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

“dati genetici”, i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

“dati biometrici”, i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

“dati relativi alla salute”, i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

“dati relativi a condanne penali e reati”, i dati personali inerenti condanne penali e reati, es. certificato casellario giudiziale (fedina penale), sentenze di condanna penali.

*****

Soggetti del trattamento:

“interessato”, la persona fisica cui si riferiscono i dati personali;

“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;

“contitolarità al trattamento – Joint Controllers”, due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento. Ciascun contitolare rimane responsabile individualmente per le attività di trattamento svolte singolarmente;

“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;

“persona autorizzata al trattamento”, colui che si occupa da vicino dell’elaborazione dei dati personali, sotto l’autorità diretta del titolare del trattamento o del responsabile del trattamento (dipendente o collaboratore, anche esterno);

“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 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.

*****

“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;

“**trattamenti effettuati per finalità amministrativo-contabili**”, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all’adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all’applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro;

Tipi di trattamento:

La **raccolta** dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento. Consiste nell'attività di acquisizione del dato.

La **registrazione** consiste nella memorizzazione dei dati su un qualsiasi supporto.

L'**organizzazion**e consiste nella classificazione dei dati secondo un metodo prescelto.

La **strutturazione** consiste nell'attività di distribuzione dei dati secondi schemi precisi.

La **conservazione** consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto.

La **consultazione** è la lettura dei dati personali. Anche la semplice visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione.

L'**elaborazione** consiste nell'attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale.

La **selezione** consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati.

L'**estrazione** consiste nell'attività di estrapolazione di dati da gruppi già memorizzati.

Il **raffronto** è un'operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione.

L'**utilizzo** è un'attività generica che ricopre qualsiasi tipo di impiego dei dati.

L'**interconnessione** consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici.

Il **blocco** consiste nella conservazione con sospensione temporanea di ogni altra operazione di trattamento.

La **comunicazione** (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata.

Per **diffusione**, invece, si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività deve ritenersi illecita.

La **cancellazione** consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici.

La **distruzione** è l'attività di eliminazione definitiva dei dati.

"limitazione di 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", 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.

*****

"archivio", qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

"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;

"stabilimento principale":

a) *per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del*

trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

"rappresentante", la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

"impresa", la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

"gruppo imprenditoriale", un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

"norme vincolanti d'impresa", le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

"autorità di controllo", l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

"autorità di controllo interessata", un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

"trattamento transfrontaliero":

a) 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 ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) 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, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

"obiezione pertinente e motivata", un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra

chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

"servizio della società dell'informazione", il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

"organizzazione internazionale", un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

*****

"sicurezza nel trattamento dei dati": *l'utilizzo di pseudonimi e la crittografia dei dati personali; la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione; la capacità di ripristinare la disponibilità e l'accesso ai dati personali in maniera tempestiva in caso di incidenti fisici o tecnici; un processo di controllo periodico e la valutazione dell'efficienza dei mezzi tecnici per verificare la sicurezza dell'elaborazione.*

*****

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni;

"**utente**", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali;

"**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico, ad esclusione delle informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

7 Ruoli, funzioni, poteri, compiti

7.1 Titolare del trattamento (TT)

Il Titolare del trattamento è la persona fisica e qualsiasi altro ente od organismo dell'organizzazione di SVILUPPO INVESTIMENTI TERRITORIO S.R.L. cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati[1] e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel caso il Titolare sia un soggetto giuridico non persona fisica, per esso opereranno, nelle diverse scelte che sia necessario assumere, i rispettivi organi apicali con funzioni decisionali, secondo le regole che disciplinano ciascun soggetto: ad esempio, il Titolare potrebbe essere l'organizzazione stessa nella persona dell'amministratore delegato, nel complesso dell'intero consiglio di amministrazione, nella figura del direttore generale o di altri dirigenti ovvero le persone fisiche che abbiano il potere di rappresentare il soggetto giuridico mediante atto di attribuzione dei poteri, delega o procura. Titolare del trattamento è il soggetto giuridico. A fronte delle delibere assunte dall'alta direzione SVILUPPO INVESTIMENTI TERRITORIO S.R.L., gli adempimenti previsti per il Titolare del trattamento sono attribuiti in capo a: DE MARCHI MONICA. I documenti, qualora necessari, che comprovano tale assunto devono essere conservati in luogo sicuro.

Il designato dal Titolare del trattamento deve:

- definire le modalità e le finalità dei trattamenti, nel rispetto dei principi normativi;
- assicurare e garantire che vengano adottate le misure di sicurezza tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta, tramite idonee istruzioni fornite per iscritto;
- vigilare sull'assolvimento e sul rispetto delle attribuzioni di funzioni e deleghe con riferimento alle nomine che ha facoltà di approvare e distribuire;

Infatti, il designato dal Titolare del trattamento, in relazione all'attività svolta, può:

- individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, i Responsabili e gli Autorizzati al trattamento e gli altri Addetti, coinvolti in operazioni collaterali non necessariamente di trattamento ma che hanno una potenziale ricaduta su di esso (es. addetti alle pulizie, ecc.).

Pertanto, tra l'altro, deve:

- dare seguito agli adempimenti prescritti ed operare nei limiti e nei modi previsti dalla norma;
- dare idoneo riscontro, senza ritardo, all'interessato che eserciti legittimamente i propri diritti, adottando idonee misure volte, in particolare:
    a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
    b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente;
- definire le modalità di resa dell'informativa all'interessato e di acquisizione del consenso, ove necessario;
- provvedere all'idonea cessazione dei trattamenti, quando necessario;

[1] Tale definizione trae spunto da quelle più stringente presente nel Codice Privacy, che è limitata ai soli dati personali.

- specificare analiticamente i compiti affidati ai Responsabili e definire l'ambito del trattamento consentito agli Autorizzati;
- vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e delle proprie istruzioni da parte dei Responsabili;
- adottare le misure di sicurezza idonee.

Qualora il designato dal Titolare del trattamento ritenga di non nominare alcun Responsabile, Autorizzato o Addetto, secondo i profili descritti nel prosieguo, ne assumerà tutte le responsabilità e funzioni.

7.1.1 Contitolarità

Qualunque trattamento di dati personali può essere svolto in contitolarità con altri soggetti. In alcuni casi la contitolarità deriva da una volontà esplicita, comune ed organizzata dei singoli soggetti titolari, che distribuiscono tra loro compiti, incarichi e misure di protezione, ma che detengono collegialmente la responsabilità delle decisioni in ordine alle finalità ed alle modalità del trattamento.

In altri casi, non esiste una reale volontà, quanto piuttosto l'adozione di una norma giuridica che impone ed attribuisce lo status di contitolare a soggetti che normalmente non operano nell'ambito del trattamento, ma che potrebbero esservi interessati e a cui va garantito il diritto di parteciparvi, trovandosi di norma in una posizione svantaggiata. Tale partecipazione si concretizza di solito con l'accesso alle informazioni, piuttosto che con l'attribuzione di un incarico di trattamento.

Dunque, nel caso in cui per lo stesso trattamento di dati, siano coinvolti più soggetti (persone fisiche, persone giuridiche, pubbliche amministrazioni, enti od organizzazioni) dotati di poteri decisionali del tutto autonomi, sia per quanto attiene alle modalità, sia alle finalità perseguite, in tal caso si definisce che tale trattamento è svolto in contitolarità e che ciascun soggetto risponde per quanto di propria competenza seppure dovendosi coordinare con gli altri per garantire il rispetto dei diritti dell'interessato.

Nei casi di trattamenti svolti in contitolarità, il Titolare del trattamento deve:

- evidenziare la situazione di contitolarità;
- promuovere la cooperazione per l'attuazione delle misure di prevenzione e protezione dai rischi che incombono sui dati;
- promuovere il coordinamento degli interventi di protezione e prevenzione dai rischi cui sono esposti i dati informandosi reciprocamente con gli altri titolari anche al fine di eliminare rischi dovuti alle interferenze.

7.2 Responsabile del trattamento (RT)

Per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti, i quali sono incardinati esternamente all'organizzazione (RT).

Il Responsabile è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati. Il Responsabile è designato dal Titolare facoltativamente, dopo essere stato individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal titolare, compreso l'ambito del trattamento affidato.

Il Responsabile deve:

- rispettare le vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, la cooperazione con il titolare per garantire all'interessato l'esercizio dei propri diritti, per il riscontro all'Autorità di Controllo e per gli adempimenti normativi, comprese l'eventuale tenuta dei Registri delle Attività di Trattamento, la valutazione di impatto, la notificazione e la comunicazione in caso di data-breach;
- effettuare il trattamento attenendosi alle istruzioni impartite dal Titolare o suo delegato;
- coordinare e vigilare sulle operazioni di trattamento svolte dagli Autorizzati che operino sotto la sua diretta autorità, affinché rispettino le istruzioni impartite e l'ambito del trattamento consentito;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Titolare o suo delegato e dalle norme vigenti;
- periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Autorizzati al trattamento dei dati personali;
- collaborare lealmente con gli altri Responsabili e con i soggetti delegati dal Titolare per il corretto funzionamento del Sistema di gestione per la protezione dei dati e la sicurezza delle Informazioni;
- informare il Titolare ovvero il soggetto delegato quale Preposto alla sicurezza del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Il Responsabile può:

- individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli Autorizzati al trattamento che operano sotto la sua autorità, fornendo adeguate istruzioni;
- compiere direttamente le operazioni di trattamento, come gli Autorizzati che operino sotto la sua diretta autorità.

7.2.1.1 Nomina del Responsabile del trattamento

La nomina del Responsabile è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

Il Responsabile a cui è stato affidato il trattamento dei dati personali all'esterno della struttura del titolare, all'atto della nomina, rilascia una dichiarazione scritta da cui risulti che adottata o si impegna ad adottare tempestivamente le misure idonee di sicurezza per il trattamento ai sensi del Codice Privacy e del disciplinare tecnico in materia di misure minime di sicurezza.

7.3 Autorizzato al trattamento (AT)

L'incaricato è la persona fisica che compie operazioni di trattamento, autorizzata dal Titolare o da un Responsabile.

La designazione[2] è facoltativa ed è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Quindi, gli Autorizzati al trattamento dei dati ricevono idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

[2] Si considera tale anche la documentata preposizione della persona fisica ad una unità o categoria per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità o categoria medesima.

Agli Autorizzati al trattamento dei dati personali può essere assegnata una parola chiave e un codice di autenticazione informatica: in tal caso è loro prescritto di adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

In particolare, gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni:

1. Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
    - La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
    - La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
    - L'Autorizzato al trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
    - In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi, altrimenti ogni sei mesi.
2. Gli Autorizzati al trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
3. Gli Autorizzati al trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
4. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli Autorizzati al trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

7.3.1.1 Nomina dell'Autorizzato al trattamento

La nomina dell'Autorizzato è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.4 Delega di funzioni

Oltre a quanto previsto dalle designazioni facoltative di responsabili ed autorizzati, sussiste la facoltà del Titolare della delega di funzioni con i seguenti limiti e condizioni:

a) che la delega risulti da atto scritto;
b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
c) che, in particolare, il delegato per esperienza, capacità ed affidabilità fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
d) che la delega attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
e) che la delega attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
f) che la delega sia accettata dal delegato per iscritto;

g) che alla delega sia data adeguata e tempestiva pubblicità.

La delega di funzioni non esclude l'obbligo di vigilanza in capo al Titolare in ordine al corretto espletamento da parte del delegato delle funzioni trasferite.

Il soggetto delegato non può, a sua volta delegare le specifiche funzioni trasferite.

7.5 Preposto al trattamento (PT)

Per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti, i quali sono incardinati internamente all'organizzazione (PT).

Il Preposto è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati. Il Preposto è designato dal Titolare facoltativamente, dopo essere stato individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. I compiti affidati al Preposto sono analiticamente specificati per iscritto dal titolare, compreso l'ambito del trattamento affidato.

Il Preposto deve:

- rispettare le vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- effettuare il trattamento attenendosi alle istruzioni impartite dal Titolare o suo delegato;
- coordinare e vigilare sulle operazioni di trattamento svolte dagli Autorizzati che operino sotto la sua diretta autorità, affinché rispettino le istruzioni impartite e l'ambito del trattamento consentito;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Titolare o suo delegato e dalle norme vigenti;
- collaborare lealmente con gli altri Preposti e Responsabili dal Titolare per il corretto funzionamento del Sistema di gestione per la protezione dei dati e la sicurezza delle Informazioni;
- informare il Titolare ovvero il soggetto delegato quale Preposto della sicurezza del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Il Preposto può:

- individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli Autorizzati al trattamento che operano sotto la sua autorità, fornendo adeguate istruzioni;
- compiere direttamente le operazioni di trattamento, come gli Autorizzati che operino sotto la sua diretta autorità.

La tenuta dei registri delle attività di trattamento, qualora non specificamente delegata al Preposto, rimane in capo al Titolare del trattamento.

7.5.1.1 Nomina del Preposto al trattamento

La nomina del Preposto è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

Il Preposto a cui è stato affidato il trattamento dei dati personali all'esterno della struttura del titolare, all'atto della nomina, rilascia una dichiarazione scritta da cui risulti che adottata o si impegna ad adottare tempestivamente le misure idonee di sicurezza per il trattamento ai sensi del Codice Privacy e del disciplinare tecnico in materia di misure minime di sicurezza.

7.6 Data Protection Officer (DPO)

Il Titolare del trattamento, in relazione all'attività svolta, può[3]/deve[4] individuare, nominare e incaricare per iscritto, un Responsabile per la protezione dei dati ovvero Data Protection Officer (DPO).

Questa figura rappresenta un elemento fondante ai fini della responsabilizzazione; la nomina del DPO facilita l'osservanza della normativa e aumenta il margine competitivo delle imprese. Oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), il DPO funge da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente, riassorbendo in sé il ruolo di RRI e RRGPA.

Il DPO non risponde personalmente in caso di inosservanza del GDPR[5].

In base all'articolo 37, paragrafo 5, il DPO "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39". Nel considerando 97 del GDPR si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

7.6.1 Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali

Ai sensi dell'articolo 38 del GDPR, il titolare del trattamento e il responsabile del trattamento assicurano che il DPO sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

È essenziale che il DPO, o il suo team di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il DPO vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni Assicurare il tempestivo e immediato coinvolgimento del DPO, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del GDPR e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il DPO sia annoverato fra gli

[3] Anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere.

[4] Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali.

[5] Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa garantire, per esempio:

- che il DPO sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del DPO riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare del trattamento o il responsabile del trattamento potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del DPO.

7.6.2 Risorse necessarie

L'articolo 38, paragrafo 2, del GDPR obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il DPO "fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del DPO da parte del senior management (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al DPO. Ciò riveste particolare importanza se viene designato un DPO interno con un contratto part-time, oppure se il DPO esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il DPO è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. È fondamentale disporre di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il DPO; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di DPO quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tale incombenze, e prevedere che il DPO stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del DPO a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al DPO supporto, informazioni e input essenziali;
- formazione permanente. I DPO devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei DPO, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro DPO (formato dal DPO stesso e dal rispettivo

personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di DPO viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di DPO sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del DPO. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

7.6.3 Indipendenza

L'articolo 38, paragrafo 3, fissa alcune garanzie essenziali per consentire ai DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile del trattamento. In particolare, questi ultimi sono tenuti ad assicurare che il DPO "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i DPO "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

Ciò significa che il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del DPO non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'articolo 39.

Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il GDPR e le indicazioni fornite dal DPO, quest'ultimo deve manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il DPO "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal DPO nel quadro delle sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento.

L'articolo 38, paragrafo 3, prevede che il DPO "non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti".

In base all'articolo 38, paragrafo 6, al DPO è consentito di "svolgere altri compiti e funzioni", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "tali compiti e funzioni non diano adito a un conflitto di interessi". L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un DPO può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un DPO non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.

7.6.4 Nomina del Data Protection Officer

La nomina del Data Protection Officer è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina può essere aggiornata o revocata in qualsiasi momento dal Titolare. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

Al titolare del trattamento o al responsabile del trattamento spetta

- di pubblicare i dati di contatto del DPO, e
- di comunicare i dati di contatto del DPO alle pertinenti autorità di controllo.

Non è necessario pubblicare anche il nominativo del DPO. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso DPO stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze. Tuttavia, comunicare il nominativo del DPO all'autorità di controllo è fondamentale affinché il DPO funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e).

7.6.5 Compiti del DPO

7.6.5.1 Sorvegliare l'osservanza del GDPR

L'articolo 39, paragrafo 1, lettera b), affida al DPO, fra gli altri, il compito di sorvegliare l'osservanza del GDPR. Nel considerando 97 si specifica che il titolare del trattamento o il responsabile del trattamento dovrebbe essere "assistito [dal DPO] nel controllo del rispetto a livello interno del presente regolamento".

Fanno parte di questi compiti di controllo svolti dal DPO, in particolare:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità;
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il DPO sia personalmente responsabile in caso di inosservanza. Il GDPR chiarisce che spetta al titolare, e non al DPO, "mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del DPO.

7.6.5.2 Approccio basato sul rischio

In base all'articolo 39, paragrafo 2, il DPO deve "considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo".

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del DPO. In sostanza, si chiede al DPO di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il DPO debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Attraverso questo approccio selettivo e pragmatico, il DPO dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

7.6.5.3 Valutazione di impatto sulla protezione dei dati

In base all'articolo 35, paragrafo 1, spetta al titolare del trattamento, e non al DPO, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o data protection by design), l'articolo 35, paragrafo 2, prevede in modo specifico che il titolare "si consulta" con il DPO quando svolge una DPIA. A sua volta, l'articolo 39, paragrafo 1, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".

Il titolare del trattamento si consulta con il DPO, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal DPO, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Inoltre, il Gruppo di lavoro raccomanda che il titolare del trattamento definisca con chiarezza, per esempio nel contratto stipulato con il DPO, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al DPO e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

7.6.5.4 Cooperazione con l'autorità di controllo e funzione di punto di contatto

In base all'articolo 39, paragrafo 1, lettere d) ed e), il DPO deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Questi compiti attengono al ruolo di "facilitatore" attribuito al DPO e già menzionato nell'introduzione alle presenti linee guida. Il DPO funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58. Si è già rilevato che il DPO è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il DPO di contattare e chiedere lumi all'autorità di controllo. L'articolo 39, paragrafo 1, prevede che il DPO possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

7.6.5.5 Relazione annuale

Il rapporto diretto tra DPO e Titolare del trattamento si esplica nella redazione di una relazione annuale delle attività svolte dal DPO da sottoporre al vertice gerarchico.

7.7 Delegato Privacy

Dal combinato disposto della nomina di Responsabile e della delega di funzioni che estende l'ambito delle funzioni e dei poteri del soggetto nominato, il sistema introduce alcune figure specifiche e peculiari che ricoprono determinati ruoli.

Qualora il soggetto con facoltà di designazione, designato dal Titolare del trattamento, ritenga di non assegnare nominativamente i seguenti ruoli, secondo i profili descritti nel prosieguo, ne assumerà tutte le responsabilità e funzioni.

7.7.1 Preposto alla sicurezza del trattamento (PST)

Il Titolare del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, un Preposto della sicurezza del trattamento che assicuri e garantisca che siano adottate le misure di sicurezza. Qualora il Titolare del trattamento ritenga di non nominare alcun Preposto della sicurezza del trattamento, ne assumerà tutte le responsabilità e funzioni.

Il Preposto alla sicurezza del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

1. Garantire che tutte le misure di sicurezza riguardanti i dati (personali e non) siano applicate.
2. Redigere ed aggiornare ad ogni variazione l'elenco delle sedi e dei locali in cui vengono trattati i dati.
3. Redigere ed aggiornare ad ogni variazione l'elenco dei trattamenti e delle banche dati e l'ambito del trattamento consentito.
4. Definire e successivamente verificare con cadenza semestrale le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito.
5. Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
6. Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
7. Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili del trattamento con il compito di individuare, nominare e incaricare per iscritto gli Autorizzati e i Preposti e sovrintendere alle operazioni di trattamento. Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Preposto al trattamento, ne assumerà tutte le responsabilità e funzioni.
8. Se il trattamento è effettuato con strumenti elettronici di elaborazione dei dati:
    a. redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
    b. individuare, nominare e incaricare per iscritto, uno o più Amministratori di Sistema, Responsabili della gestione e della manutenzione degli strumenti elettronici;
    c. individuare, nominare e incaricare per iscritto, uno o più Autorizzati della custodia delle copie delle credenziali qualora vi sia più di un Autorizzato al trattamento;
    d. individuare, nominare e incaricare per iscritto, uno o più Autorizzati delle copie di sicurezza delle banche dati, anche con il compito di custodire e conservare i supporti utilizzati per le copie dei dati;
    e. redigere ed aggiornare ad ogni variazione l'elenco dei soggetti nominati quali Responsabili della gestione e della manutenzione degli strumenti elettronici, Amministratori di Sistema, Autorizzati della custodia delle copie delle credenziali e Autorizzati delle copie di sicurezza delle banche dati;

f. verificare, con cadenza almeno annuale, l'attività svolta da Responsabili della gestione e della manutenzione degli strumenti elettronici, Amministratori di Sistema, Autorizzati della custodia delle copie delle credenziali e Autorizzati delle copie di sicurezza delle banche dati, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;

9. Sovrintendere al buon funzionamento e applicazione del sistema di gestione per la protezione dei dati e sicurezza delle informazioni, provvedendo a:
    a. definire le strategie e le risorse relative all'impostazione del sistema di gestione;
    b. fornire indicazioni alle Risorse Umane circa il funzionamento del sistema e la sua applicazione in SVILUPPO INVESTIMENTI TERRITORIO S.R.L.;
    c. acquisire e analizzare dati statistici (con particolare riferimento agli indicatori di efficienza ed efficacia);
    d. monitorare l'andamento delle attività e riportare periodicamente al Titolare circa lo stato del Sistema;
    e. effettuare gli audit interni e assistere eventuali valutatori in occasione degli audit esterni;
    f. garantire la conservazione e l'archiviazione della documentazione del sistema e imposta dai regolamenti;
    g. gestire Non Conformità e curare e presidiare la pianificazione e attuazione di Azioni Correttive e Preventive.

In particolare, il Preposto alla sicurezza del trattamento con riferimento a quei dati che rientrano nell'ambito applicativo del Codice Privacy e che siano trattati con strumenti elettronici, vista la particolare criticità del ruolo di Amministratori di Sistema, Responsabili della Strumentazione elettronica, Autorizzati della custodia delle copie delle credenziali e Autorizzati delle copie di sicurezza delle banche dati deve:

g. adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema;
h. valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.

7.7.1.1 Nomina del Preposto alla sicurezza del trattamento

La nomina del Preposto alla sicurezza del trattamento è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal Titolare senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.7.2 Preposto al riscontro all'interessato (PRI)

Il Titolare del trattamento, in relazione all'attività svolta, quando non è stato designato il Data Protection Officer (DPO), può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Preposti al riscontro all'interessato.

Qualora il Titolare del trattamento ritenga di non nominare alcun Preposto al riscontro all'interessato, ne assumerà tutte le responsabilità e funzioni.

Il Preposto al riscontro all'interessato è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

1. rispondere prontamente alle richieste degli interessati, in esecuzione di quanto disposto dagli artt. 7, 8, 9 e 10 del Codice Privacy e comunque rendere agli interessati tutte le informazioni prescritte dalla legge.

7.7.2.1 Nomina del Preposto al riscontro all'interessato

La nomina del Responsabile è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.7.3 Preposto al riscontro al Garante e alla Pubblica Amministrazione (PRGPA)

Il Titolare del trattamento, in relazione all'attività svolta, quando non è stato designato il Data Protection Officer (DPO), può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Preposti del riscontro al Garante e alla Pubblica Amministrazione.

Qualora il Titolare del trattamento ritenga di non nominare alcun Preposto del riscontro al Garante, ne assumerà tutte le responsabilità e funzioni.

Il Preposto del riscontro al Garante è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

1. rappresentare il Titolare in ogni atto con e/o nei confronti dei privati, del Garante e di ogni altro possibile organo della Pubblica Amministrazione nell'ambito della materia della tutela dei dati personali, del loro trattamento e della sicurezza delle informazioni;
2. interagire con il Garante nel caso di effettuazione di controlli e accessi da parte della suddetta autorità e rispondere ad ogni sua richiesta di informazioni, salva naturalmente la difesa dei diritti e degli interessi legittimi del Titolare; e così, ad esempio,
    a. "fornire le informazioni od esibire i documenti richiesti" dal Garante;
    b. comunicare al Garante le "necessarie informazioni" richieste;
    c. adoperarsi affinché siano adottate le misure e gli accorgimenti a garanzia dell'interessato, eventualmente prescritti nei provvedimenti del Garante.

7.7.3.1 Nomina del Preposto al riscontro al Garante e alla Pubblica Amministrazione

La nomina del Preposto è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.8 Soggetti che si occupano di strumenti elettronici di supporto al trattamento dei dati

7.8.1 Amministratore di sistema (ADS)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Amministratori di sistema[6].

[6] Con i provvedimenti del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009)e del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Amministratore di sistema, ne assumerà tutte le responsabilità e funzioni.

L'Amministratore di sistema è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende al buon funzionamento di banche di dati e di sistemi software complessi.

È compito dell'Amministratore di sistema:

1. sovrintendere al buon funzionamento di banche di dati e di sistemi software complessi
2. proteggere le banche dati e i sistemi software complessi dal rischio di intrusione o di accesso non autorizzato
3. attivare le credenziali di autenticazione di accesso alle banche di dati e ai sistemi software complessi rientranti nel proprio ambito di competenza e attivare ove possibile e previsto le politiche di autorizzazione agli Autorizzati al trattamento, su indicazione del Preposto alla sicurezza del trattamento ovvero del Responsabile del trattamento
4. adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema stessi
5. Informare il Preposto alla sicurezza del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Pertanto, con la definizione di Amministratore di Sistema si individuano:

- figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (così come avviene generalmente in ambito informatico)
- altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici. Pertanto, gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup e recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti in chiaro le informazioni medesime.

7.8.1.1 Criticità del ruolo di Amministratore di Sistema

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice

attribuzioni delle funzioni di amministratore di sistema e alla proroga dei termini per il loro adempimento, il Garante per la protezione dei dati personali ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies).

Le funzioni tipiche dell'amministrazione di un sistema che tratti dati personali sono richiamate nel menzionato Allegato B del Codice Privacy, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione. Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta.

7.8.1.2 Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale Autorizzato al trattamento (ai sensi dell'art. 30 del Codice Privacy) ci si deve attenere comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili del trattamento (ai sensi dell'art. 29 del Codice Privacy).

7.8.1.3 Registrazione degli accessi degli amministratori di sistema

Le registrazioni degli accessi logici (access log) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, mediante idonei sistemi di autenticazione informatica, devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica 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 185 giorni (sei mesi).

7.8.1.4 Verifica periodica dell'attività svolta

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Preposto alla sicurezza del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

7.8.1.5 Nomina dell'Amministratore di Sistema

La nomina dell'Amministratore di Sistema è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato, con la specificazione di quali banche di dati e sistemi software complessi siano da sovrintendere e con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, deve essere in ogni caso individuale e può essere aggiornata o revocata in qualsiasi momento dal soggetto designante senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.8.2 Responsabile della gestione e della manutenzione degli strumenti elettronici (RGSE)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici.

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Responsabile della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è un Amministratore di sistema (persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che sovrintendere al buon funzionamento delle risorse del sistema informativo e si occupa specificatamente dei sistemi di elaborazione e dei relativi sistemi operativi.

È compito dei Responsabili della gestione e della manutenzione degli strumenti elettronici:

1. Sovrintendere agli strumenti di un sistema informativo, con finalità atte alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti
2. Attivare le credenziali di autenticazione di accesso agli strumenti di elaborazione e attivare ove possibile e previsto le politiche di autorizzazione agli Autorizzati al trattamento, su indicazione del Preposto alla sicurezza del trattamento ovvero del Responsabile del trattamento.
3. Definire quali politiche adottare per la protezione dei sistemi contro virus informatici, malware, trojan, spyware, ecc. e verificarne l'efficacia con cadenza almeno semestrale.
4. Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di hackers).
5. Informare il Preposto alla sicurezza del trattamento nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati.

7.8.2.1 Nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la descrizione dell'ambito del trattamento affidato, specificando gli elaboratori che è chiamato a sovrintendere, deve essere in ogni caso individuale e può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.8.3 Autorizzato della custodia delle copie delle credenziali (ICCC)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Autorizzati della custodia delle copie delle credenziali.

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Autorizzato della custodia delle copie delle credenziali, ne assumerà tutte le responsabilità e funzioni.

L'Autorizzato della custodia delle copie delle credenziali è un Amministratore di sistema (persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che sovrintende al sistema di autenticazione centralizzato degli elaboratori del sistema informativo, delle banche dati o dei sistemi software complessi che sovrintende. In taluni casi può coincidere con il Responsabile della gestione e della manutenzione degli strumenti elettronici.

È compito dell'Autorizzato della custodia delle copie delle credenziali:

1. Gestire e custodire le credenziali per l'accesso ai dati degli Autorizzati al trattamento.
2. Qualora non sussista un sistema di autenticazione centralizzato, predisporre, per ogni Autorizzato al trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto.
3. Nel caso si utilizzi un sistema di autenticazione centralizzato, non è necessario predisporre le buste per gli incaricati, in quanto si utilizzano le funzioni del sistema stesso. È tuttavia necessario predisporre la busta con l'indicazione della credenziale di autenticazione dell'utente con i privilegi

di amministrazione (es. root, Administrator) che ha facoltà di creare, modificare, sospendere e rimuovere le credenziali stesse.
4. Istruire gli Autorizzati al trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
5. Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
6. Revocare le credenziali per l'accesso ai dati degli Autorizzati al trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi.

7.8.3.1 Nomina dell'Autorizzato della custodia delle copie delle credenziali

La nomina dell'Autorizzato della custodia delle copie delle credenziali è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e la specificazione del sistema di autenticazione a cui l'incaricato è preposto, deve essere in ogni caso individuale e può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.8.4 Autorizzato delle copie di sicurezza delle banche dati (ICSBD)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Autorizzati delle copie di sicurezza delle banche dati.

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Autorizzato delle copie di sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

L'Autorizzato delle copie di sicurezza delle banche dati è un Amministratore di sistema (persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che provvede alle misure per le copie di sicurezza periodiche dei dati presenti sugli elaboratori del sistema informativo, sui sistemi software complessi o delle banche dati in gestione. In taluni casi può coincidere con il Responsabile della gestione e della manutenzione degli strumenti elettronici.

È compito dell'Autorizzato delle copie di sicurezza delle banche dati:

1. Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Preposto alla sicurezza dei dati personali.
2. Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
3. Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
4. Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
5. Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

7.8.4.1 Nomina dell'Autorizzato delle copie di sicurezza delle banche dati

La nomina dell'Autorizzato delle copie di sicurezza delle banche dati è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni per le copie di sicurezza periodiche, deve essere in ogni caso individuale e può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.8.5 Autorizzati della manutenzione o assistenza su particolari strumenti o programmi elettronici, senza qualifica di Amministratori di sistema (IMTZ)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Autorizzati della manutenzione o assistenza su particolari strumenti o programmi elettronici, senza qualifica di Amministratori di sistema.

L'Autorizzato della manutenzione o assistenza su particolari strumenti o programmi elettronici non è qualificato come Amministratore di sistema.

L'Autorizzato della manutenzione o assistenza su particolari strumenti elettronici, banche dati o sistemi software complessi è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che provvede ad effettuare operazioni di manutenzione ed assistenza su strumenti e programmi che contengono dati, con un'autorizzazione di accesso ai dati limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di manutenzione e/o assistenza e comunque sotto la supervisione del Preposto alla sicurezza del trattamento.

7.8.5.1 Nomina dell'Autorizzato della manutenzione o assistenza su particolari strumenti elettronici

La nomina dell'Autorizzato della manutenzione o assistenza su particolari strumenti elettronici è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina, contenente le istruzioni e l'indicazione delle operazioni di manutenzione ed assistenza e degli strumenti e dei programmi oggetto dell'incarico può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.9 Soggetti che non trattano dati

Esistono inoltre alcune figure professionali che, seppur non coinvolte necessariamente con il trattamento, possono potenzialmente entrare in contatto con i supporti di memorizzazione e archiviazione dei dati o con gli strumenti elettronici di elaborazione. Pertanto, occorre che tali soggetti siano adeguatamente informati dei loro compiti, obblighi e divieti.

7.9.1 Addetto al controllo dei locali (ACL)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Addetti al controllo dei locali, anche senza qualifica aggiuntiva di Autorizzati al trattamento.

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Addetto al controllo dei locali, ne assumerà tutte le responsabilità e funzioni.

L'Addetto al controllo dei locali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che provveda a controllare periodicamente e direttamente i sistemi, le apparecchiature e le dotazioni di sicurezza per l'accesso ai locali assegnati e per la conservazione dei dati ivi contenuti, allo scopo di prevenire e per quanto possibile impedire intrusioni, furti o danneggiamenti.

L'addetto non ha responsabilità circa eventuali mancanze organizzative o strutturali; l'incarico rappresenta una richiesta di coinvolgimento dell'addetto, volta alla sua sensibilizzazione e con il fine di migliorare l'efficienza del sistema di protezione dei dati personali.

Quando presente nei locali assegnatigli, è compito dell'Addetto al controllo dei locali:

1. tentare di impedire l'intrusione nei locali stessi da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento;
2. tentare di impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia dei dati da parte di persone non autorizzate, secondo quanto stabilito dal Responsabile del trattamento;
3. nel caso sia previsto dalle procedure di sicurezza, identificare e registrare i soggetti ammessi all'accesso dopo l'orario di chiusura dei locali stessi ed eventualmente anche durante l'orario di apertura;
4. verificare che le dotazioni (stanze, armadi, cassettiere, scatole, contenitori vari, ecc.) per la conservazione sicura dei documenti e delle informazioni, quando necessarie, siano muniti di serratura.

7.9.1.1 Nomina dell'Addetto al controllo dei locali

La nomina dell'Addetto al controllo dei locali è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

7.9.2 Addetti alla sorveglianza e vigilanza (ASV)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Addetti alla sorveglianza e vigilanza, anche senza qualifica aggiuntiva di Autorizzati al trattamento, eventualmente specificando l'ambito di operatività (es. sede, locali, ecc.).

L'Addetto alla sorveglianza e vigilanza è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che, provvedendo alla sorveglianza dell'immobile, ovvero di una sua parte o locali o del suo perimetro, ed una supervisione e vigilanza degli accadimenti che avvengono all'interno dell'area dello stabile. Le attività che l'Addetto è chiamato a svolgere possono consistere:

- nel controllo delle infrastrutture di servizio, della chiusura delle porte e delle finestre, dei quadri elettrici delle attrezzature elettroniche;
- nella registrazione dei visitatori, nel controllo e nell'ispezione degli accessi;
- nella regolarizzazione dell'afflusso delle vetture ai parcheggi;
- nel monitoraggio dell'impianto d'allarme antintrusione e nell'obbligo, in caso di allarme, di darne immediata notizia al servizio tecnico e ai soggetti individuati dal proprietario dell'immobile o dall'amministrazione per i necessari interventi;
- nei compiti ispettivi sia nel parcheggio che in aree interne dell'edificio;
- nell'impedire l'ingresso ad accattoni, venditori ambulanti o persone sospette;
- nell'impedire il volantinaggio di persone non autorizzate;
- nella gestione tecnica del patrimonio mobiliare ed immobiliare dell'Azienda;
- nello svolgere uno specifico lavoro di prevenzione ed eventuale intervento antincendio, antiallagamento, fughe di gas e gestione delle emergenze;
- altre mansioni definite in Sede.

Pertanto, potrebbe entrare a conoscenza dei dati e in contatto dei supporti che li contengono o degli strumenti che li trattano, determinando un rischio contestuale per la riservatezza e sicurezza dei dati.

Eventualmente, unitamente alla qualifica di Autorizzato al trattamento, ulteriori attività potrebbero consistere:

- nel custodire le cose loro consegnate e fornire indicazioni;
- nel distribuire la corrispondenza ordinaria;
- nel rispondere al centralino e smistare le chiamate a chi di competenza;

È compito dell'Addetto alla sorveglianza e vigilanza, quando trattasi di soggetto che organizza il servizio impiegando personale terzo:

1. Comunicare i dati per l'identificazione e registrazione delle persone che abitualmente svolgono le operazioni di sorveglianza e vigilanza nei locali contenenti dati (prima e dopo l'orario di chiusura) per considerarle autorizzate all'accesso.
2. In caso di assenza o impedimento delle persone che abitualmente svolgono le operazioni di alla sorveglianza e vigilanza nei locali contenenti dati, comunicare tempestivamente e ad ogni occasione i nominativi dei sostituti.
3. Tenere un registro delle persone autorizzate ad accedere ai locali.
4. Informare il personale addetto alle operazioni di alla sorveglianza e vigilanza nei locali contenenti dati circa l'obbligo di limitare le proprie attività ai soli compiti assegnati e, in particolare che:
    - non dovrà essere consultato nessun documento, né archivio;
    - l'uso delle apparecchiature informatiche è vietato.

È compito dell'Addetto alla sorveglianza e vigilanza, quando trattasi di persona direttamente impegnata nello svolgimento del servizio, senza delega a terzi

1. Comunicare i propri dati per l'identificazione e registrazione al fine dell'autorizzazione all'accesso.
2. In caso di propria assenza o impedimento, comunicare tempestivamente e ad ogni occasione il nominativo dell'eventuale sostituto.
3. Svolgere le proprie attività limitandosi ai soli compiti assegnati, tenendo conto che, in particolare;
    - non dovrà essere consultato nessun documento, né archivio;
    - l'uso delle apparecchiature informatiche è vietato.

7.9.3 Addetti alle pulizie e manutenzioni ordinarie (APLZ)

Il Preposto alla sicurezza del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Addetti alle pulizie e manutenzioni ordinarie, anche senza qualifica aggiuntiva di Autorizzati al trattamento, eventualmente specificando l'ambito di operatività (es. sede, locali, ecc.).

Qualora il Preposto alla sicurezza del trattamento ritenga di non nominare alcun Addetto alle pulizie e manutenzioni ordinarie, assumerà tutte le responsabilità del caso.

L'Addetto alle pulizie e manutenzioni ordinarie è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che, provvedendo alla pulizia dei locali ovvero alla manutenzione ordinaria di impianti e strumenti presenti nei locali che non comportino un diretto trattamento di dati, potrebbe entrare a conoscenza dei dati e in contatto dei supporti che li contengono o degli strumenti che li trattano, determinando un rischio contestuale per la riservatezza e sicurezza dei dati.

È compito dell'Addetto alle pulizie e manutenzioni ordinarie, quando trattasi di soggetto che organizza il servizio impiegando personale terzo:

5. Comunicare i dati per l'identificazione e registrazione delle persone che abitualmente svolgono le operazioni di pulizia o manutenzione ordinaria nei locali contenenti dati (prima e dopo l'orario di chiusura) per considerarle autorizzate all'accesso.

6. In caso di assenza o impedimento delle persone che abitualmente svolgono le operazioni di pulizia o manutenzione ordinaria nei locali contenenti dati, comunicare tempestivamente e ad ogni occasione i nominativi dei sostituti.
7. Tenere un registro delle persone autorizzate ad accedere ai locali.
8. Informare il personale addetto alle operazioni di pulizia o manutenzione ordinaria nei locali contenenti dati circa l'obbligo di limitare le proprie attività ai soli compiti assegnati e, in particolare che:
    - non dovrà essere consultato nessun documento, né archivio;
    - l'uso delle apparecchiature informatiche è vietato;
    - il materiale cartaceo asportato, destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire.

È compito dell'Addetto alle pulizie e manutenzioni ordinarie, quando trattasi di persona direttamente impegnata nello svolgimento del servizio, senza delega a terzi

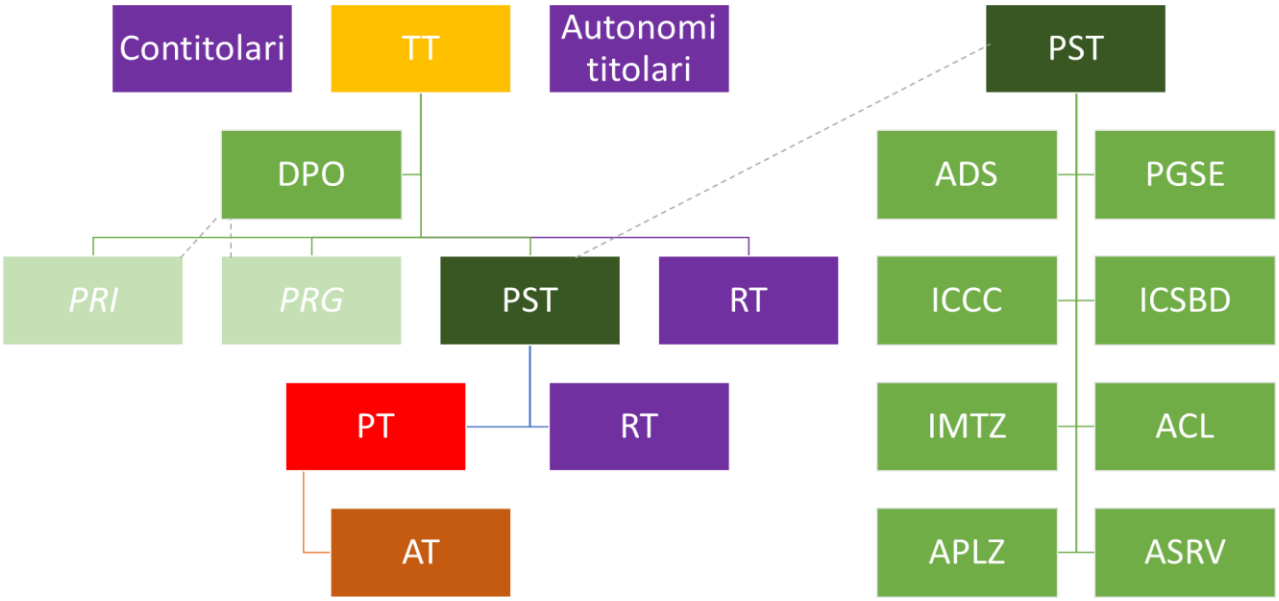
4. Comunicare i propri dati per l'identificazione e registrazione al fine dell'autorizzazione all'accesso
5. In caso di propria assenza o impedimento, comunicare tempestivamente e ad ogni occasione il nominativo dell'eventuale sostituto.
6. Svolgere le proprie attività limitandosi ai soli compiti assegnati, tenendo conto che, in particolare;
    - non dovrà essere consultato nessun documento, né archivio;
    - l'uso delle apparecchiature informatiche è vietato;
    - il materiale cartaceo asportato, destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire.

7.9.3.1 Nomina dell'Addetto alle pulizie e manutenzioni ordinarie

La nomina dell'Addetto alle pulizie e manutenzioni ordinarie è a tempo indeterminato, salvo diversa specificazione, e decade per revoca o dimissioni. La nomina può essere aggiornata o revocata in qualsiasi momento dal Preposto alla sicurezza del trattamento senza preavviso. L'atto di nomina controfirmato per accettazione dal soggetto designato deve essere conservato secondo procedura.

8 Organigramma

Sulla base dei ruoli descritti in precedenza è possibile delineare il seguente organigramma di massima. Per ciascun nodo, a pari livello, il ruolo può essere ricoperto da uno o più soggetti; in assenza di assegnazioni per un dato nodo, i soggetti al livello superiore ne assumono compiti, funzioni e responsabilità.



Legenda:

- TT=Titolare del trattamento
  - DPO=Data Protection Officer
  - PRI=Preposto al riscontro all'interessato (può essere designato solo in assenza di DPO)
  - PRG= Preposto al riscontro al Garante e alla Pubblica Amministrazione (può essere designato solo in assenza di DPO)
  - PST=Preposto alla sicurezza del trattamento (interno all'organizzazione)
    - ADS=Amministratore di sistema
    - PGSE=Preposto alla gestione e della manutenzione degli strumenti elettronici
    - ICCC=Incaricato della custodia delle copie delle credenziali di autenticazione
    - ICSBD=Incaricato delle copie di sicurezza delle banche dati
    - IMTZ=Incaricato della manutenzione o assistenza su particolari strumenti o programmi elettronici, senza qualifica di Amministratori di sistema
    - ACL=Addetto al controllo dei locali
    - APLZ=Addetto alle pulizie e manutenzioni ordinarie
    - ASRV=Addetto alla sorveglianza e vigilanza
- PT=Preposto al trattamento (può essere designato da TT o PST)
- AT=Autorizzato al trattamento (può essere designato da TT o PST o PT)
- RT=Responsabile del trattamento (esterno all'organizzazione; può essere designato da TT o PST)

9 Documentazione del sistema

Oltre a codesto documento che dà una descrizione generale del Modello organizzativo per la protezione dei dati e per la sicurezza delle informazioni, sono predisposti ulteriori documenti che rappresentano sia la descrizione e l'implementazione delle misure organizzative procedurali, sia obblighi normativi.

Pertanto, gli ulteriori documenti che compongono il sistema sono:

9.1 Registri estesi delle attività di trattamento (REAT)

Con l'acronimo REAT, che corrisponde ai "Registri estesi delle attività di trattamento", si intende quell'elenco, tenuto in forma scritta, raggruppato per ciascuna attività di trattamento, che comprende tanto le informazioni previste all'art.30 co.1-2 quanto altre utili ad una completa analisi e disamina ai fini del rispetto del GDPR.

I Registri estesi delle attività di trattamento sono redatti in conformità all'art.30 del GDPR anche ove non trovasse riscontro l'obbligo della loro tenuta in virtù della deroga di cui al co.5 del medesimo articolo. Le informazioni ivi previste sono eventualmente integrate per attestare informazioni ovvero evidenze in merito ad altri obblighi e adempimenti di cui all'intero GDPR ovvero di altre norme cogenti applicabili. In particolare, vi sono: una breve descrizione dell'attività, le misure generali e quelle relative alle singole sedi fisiche (suddivise per aree), il dettaglio dei singoli trattamenti.

I registri sono revisionati periodicamente e tenuti aggiornati.

Le attività di trattamento prese in considerazione nei REAT sono:

- Direzione
- Gestione amministrativo-contabile
- Selezione del personale
- Gestione del rapporto di lavoro nei confronti dei propri lavoratori
- Gestione attività di segreteria generale
- Gestione commerciale e marketing
- Gestione acquisti e approvvigionamenti
- Adempimenti per antiriciclaggio
- Sistema di gestione della sicurezza sul lavoro
- Sistema di gestione della protezione del trattamento di dati
- Sistema di gestione di prevenzione dei reati presupposto di cui al D.Lgs. 231/2001
- Sistema informatico e di telecomunicazioni
- Sito web e newsletter

♦ SVILUPPO INVESTIMENTI TERRITORIO SRL

9.2 Report sull'adozione del GDPR

Il "Report sull'adozione del GDPR" contiene le ulteriori indicazioni e prescrizioni, complementari a quelle indicate nei REAT, relativamente agli adempimenti previsti dal Regolamento europeo sulla protezione dei dati a partire dal Principio di responsabilizzazione (art. 5 co.2) e proseguendo con:

- Liceità dei trattamenti (artt. 6, 9, 10)
- Informazioni all'interessato - informative (artt. 12-14)
- Registrazione del consenso (artt. 7, 8)
- Comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (artt. 11, 12, 15-22, 34)
- Misure tecniche e organizzative (art. 24, 25, 32)
- Dimostrazione di conformità (art.24)
- Soggetti coinvolti nel trattamento e per la protezione dei dati (artt.26-29, 37)
- Ente come Titolare del trattamento (art.4)
- Ente come Responsabile del trattamento (art.4)
- Contitolari del trattamento (art. 26)
- Rappresentante nell'Unione Europea (art. 27)
- Responsabile della protezione dei dati – DPO (art. 37)
- Responsabili del trattamento (art.28)
- Autorizzati al trattamento (art. 29)
- Preposti al trattamento (art. 29)
- Cooperazione con l'autorità di controllo (art. 31, 58)
- Violazione dei dati personali (artt. 33, 34)
- Valutazione d'impatto sulla protezione dei dati (art. 35)
- Consultazione preventiva (art. 36)
- Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali (artt. 44-49)
- Trasferimento sulla base di una decisione di adeguatezza (art. 45)
- Trasferimento soggetto a garanzie adeguate (art. 46)
- Trasferimento in deroga (art. 49)

Il report è revisionato periodicamente e tenuto aggiornato.

9.3 Accordi, incarichi e designazioni

Si intendono nomine, designazioni, incarichi, contratti e accordi relativi al Regolamento (UE) 2016/679.

9.4 Ulteriori evidenze documentali

Ad esempio:

- Attestazione della legittimità dei trasferimenti di dati Extra-UE, come decisioni di adeguatezza o contratti con clausole contrattuali standard;

- Modelli di informativa
- Registro delle Richieste e delle Comunicazioni con l'Interessato
- Registro delle Violazioni dei dati
- Registri ed attestati di formazione
- Documentazione tecnica e attestazioni di garanzia dei fornitori/installatori/noleggiatori dei sistemi elettronici di trattamento
- Procedure ed istruzioni operative
- Altre evidenze di altri sistemi di gestione (es. ISO9001, ISO27001, ecc.)
- Ecc.

10 Mansionario riferito ai trattamenti di dati personali svolti internamente

Ad integrazione di quanto specificato nella sezione 7 su "Ruoli, funzioni, poteri, compiti", tenuto conto dei delle attività di trattamento così come descritte nei REAT, è stabilito il seguente mansionario, anche con il fine di impostare, determinare e comunicare l'ambito del trattamento consentito delle varie categorie omogenee di soggetti che trattano i dati. Le categorie omogenee di soggetti autorizzati al trattamento sono:

- IMPIEGATI
- TITOLARE

10.1 Categoria: IMPIEGATI

10.1.1 Ambito Autorizzato al trattamento

Con riferimento al Regolamento Generale sulla Protezione dei Dati, Reg.(UE) 2016/679 e in considerazione di quanto in esso prescritto circa gli adempimenti e le misure di sicurezza da adottare, il soggetto è autorizzato al trattamento dei dati personali nell'ambito della propria attività lavorativa per la categoria omogenea di soggetti autorizzati al trattamento.
La persona designata, nell'ambito delle operazioni eseguite, è autorizzata a trattare, per conto di SVILUPPO INVESTIMENTI TERRITORIO S.R.L., i dati personali necessari nonché a svolgere tutte le operazioni di trattamento necessarie per assolvere la propria mansione, i propri compiti e la propria funzione relativamente alle categorie omogenee di trattamento cui è assegnata ed ai seguenti specifici trattamenti, così come definiti internamente al soggetto giuridico scrivente, con le eventuali limitazioni e/o specificazioni del caso.

Trattamento n.1: Sistema di gestione della sicurezza sul lavoro

Descrizione (ovvero a riguardo di):

Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di Legge (spec. D.Lgs. 81/08).

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro
- Esigenze di natura organizzativa e produttiva
- Medicina del lavoro e valutazione della capacità lavorativa del dipendente
- Sicurezza e tutela dell'incolumità delle persone
- Salute e sicurezza sul lavoro
- Adempimento di un obbligo legale al quale è soggetto l'ente

I dati personali trattati sono:

- personali
- documenti di identità
- relativi alla salute (per la sorveglianza sanitaria e la relativa idoneità al lavoro)
- antropometrici (es. peso, altezza, ecc.) (nel caso di valutazioni ergonomiche)
- immagini personali (nel caso dei tesserini di riconoscimento o per la formazione)

- relativi a comportamenti illeciti o fraudolenti (nel caso di segnalazioni di violazioni delle norme di legge)

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: Sistema di gestione della protezione del trattamento di dati

Descrizione (ovvero a riguardo di):

Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di Legge.

Gli scopi del trattamento sono:

- Adempimento di un obbligo legale al quale è soggetto l'ente

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- fornitori
- terzi identificati e identificabili (nell'esercizio dei diritti degli interessati)

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.3: SVILUPPO INVESTIMENTI TERRITORIO SRL

Descrizione (ovvero a riguardo di):

.

Gli scopi del trattamento sono:

- Attività amministrativo – contabili (connesse allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale)
- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso
- Attività commerciale

I dati personali trattati sono:

- personali
- personali economici

La persona autorizzata al trattamento

♦ Può trattare i dati personali contenuti nei documenti affidati nello svolgimento della sua attività nonché quelli contenuti in archivi cartacei, informatici o comunque costituiti, anche mediante l'utilizzo di strumenti elettronici. L'incaricato deve usare la massima riservatezza e discrezione nella tenuta dei dati di cui sopra e la massima diligenza nella conseguente loro protezione.

♦ Ha facoltà di utilizzare gli asset tecnologici in dotazione (dispositivi elettronici come quelli di rete o servizi specifici ecc.) per lo svolgimento dei compiti assegnati e per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute dal Titolare o dal Responsabile scrivente e anche dal delegante.

Al soggetto autorizzato può essere data la facoltà di utilizzare propri strumenti elettronici che prevedano anche operazioni di trattamento di dati personali, purché garantisca che tali dati non siano conservati o che siano cancellati al termine dell'uso o comunque protetti in settori cifrati e ad accesso ristretto al solo autorizzato.

Nella regolamentazione interna, parte integrante delle istruzioni e disposizioni a cui ogni persona autorizzata al trattamento deve conformarsi, è puntualmente individuato per ciascuna unità di appartenenza l'ambito del trattamento consentito.

10.2 Categoria: TITOLARE

10.2.1 Ambito Preposto delegato dal Titolare del trattamento

Con riferimento al Regolamento Generale sulla Protezione dei Dati, Reg.(UE) 2016/679 e in considerazione di quanto in esso prescritto circa gli adempimenti e le misure di sicurezza da adottare, la persona individuata quale preposto al trattamento dei dati personali nell'ambito della propria attività lavorativa per la categoria omogenea di soggetti autorizzati al trattamento, agisce per conto di SVILUPPO INVESTIMENTI TERRITORIO S.R.L. con il compito di sovrintendere alle operazioni di trattamento di seguito riportate.

Il preposto, nell'ambito dei trattamenti da sovrintendere, è anche autorizzato a trattare, per conto dell'ente scrivente, i dati personali necessari nonché a svolgere tutte le operazioni di trattamento necessarie per assolvere la propria mansione, i propri compiti e la propria funzione relativamente alle categorie omogenee di trattamento cui è assegnata ed ai seguenti specifici trattamenti, così come definiti internamente nei REAT, con le eventuali limitazioni e/o specificazioni del caso.

Trattamento n.1: Direzione

Descrizione (ovvero a riguardo di):

Definizione di politiche,strategie
Controllo e riesame periodico
Dati, valutazioni e considerazioni su lavoratori, clienti, fornitori, professionisti e terzi
Contenziosi giudiziali e stragiudiziali per cause civili, penali, di lavoro, amministrative.

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro
- Esigenze di natura organizzativa e produttiva

- Gestione logistica

I dati personali trattati sono:

- personali

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: Gestione amministrativo-contabile

Descrizione (ovvero a riguardo di):

Fatture, parcelle, corrispettivi, multe, movimenti contabili, modelli fiscali, tributari, doganali, ecc. Predisposizione dichiarazione dei redditi e bilancio. Documenti vari necessari al corretto adempimento delle misure di Legge in materia societaria, fiscale e tributaria

Estratti conti, bonifici, assegni, versamenti, riba, rid, ecc.

Solleciti ai clienti per il pagamento di effetti scaduti

Informazioni commerciali sul credito e la solvibilità

Informazioni necessarie per la gestione delle polizze assicurative di cui si è contraente e/o beneficiario, ecc..

Gli scopi del trattamento sono:

- Attività amministrativo – contabili (connesse allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale)
- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso

I dati personali trattati sono:

- personali
- personali economici
- informazioni per disporre pagamenti

L**e categorie di persone interessate sono:**

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.3: Selezione del personale

Descrizione (ovvero a riguardo di):

Curriculum vitae, questionari, prove di selezione di candidati per posti di lavoro.

Gli scopi del trattamento sono:

- Selezione del personale

I dati personali trattati sono:

- personali
- documenti di identità
- (Curriculum Vitae e annotazioni di eventuale colloquio)

L**e categorie di persone interessate sono:**

- candidati lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.4: Gestione del rapporto di lavoro nei confronti dei propri lavoratori

Descrizione (ovvero a riguardo di):

Relazioni con i propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese la registrazione delle presenze, l'elaborazione dei compensi, la gestione del libro unico del lavoro, i rapporti con enti previdenziali, assicurativi, sindacali, ecc.

Dati inerenti alle presenze dei propri lavoratori (dipendenti, soci, amministratori, collaboratori), comprese le ferie, le malattie, i lutti, i permessi, gli straordinari, ecc.

Visite ed esami di medicina del lavoro svolte dai propri lavoratori soggetti

Contenziosi giudiziali e stragiudiziali per contenziosi di lavoro.

Gli scopi del trattamento sono:

- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso
- Adempimenti connessi al rapporto di lavoro in tutte le sue fasi (assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi e l'esercizio dei diritti stabiliti dalla legge o da contratti collettivi in applicazione delle norme in materia di diritto del lavoro, della sicurezza sociale e protezione sociale, sindacale, previdenziale-assistenziale; parità e diversità sul posto di lavoro; esercizio e godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro; cessazione del rapporto di lavoro)
- Salute e sicurezza sul lavoro
- Medicina del lavoro e valutazione della capacità lavorativa del dipendente

I dati personali trattati sono:

- personali
- documenti di identità
- informazioni per disporre pagamenti
- personali economici

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori
- familiari dei lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.5: Gestione attività di segreteria generale

Descrizione (ovvero a riguardo di):

Mittente, destinatari, contenuto delle e-mail certificate

Documenti di trasporto, indirizzari, ecc.

Attività da svolgere, eventualmente con soggetti terzi, in orari e giorni specifici

Informazioni varie conservate a fini amministrativi o per future ed eventuali pratiche legali.

Gli scopi del trattamento sono:

- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso
- Attività amministrativo – contabili (connesse allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale)

I dati personali trattati sono:

- personali
- personali economici

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori
- clienti
- fornitori
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.6: Sistema di gestione della sicurezza sul lavoro

Descrizione (ovvero a riguardo di):

Documenti vari necessari al corretto adempimento delle misure di sicurezza, come previsto anche da norme di Legge (spec. D.Lgs. 81/08).

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro
- Esigenze di natura organizzativa e produttiva
- Medicina del lavoro e valutazione della capacità lavorativa del dipendente
- Sicurezza e tutela dell'incolumità delle persone
- Salute e sicurezza sul lavoro
- Adempimento di un obbligo legale al quale è soggetto l'ente

I dati personali trattati sono:

- personali
- documenti di identità
- relativi alla salute (per la sorveglianza sanitaria e la relativa idoneità al lavoro)
- antropometrici (es. peso, altezza, ecc.) (nel caso di valutazioni ergonomiche)
- immagini personali (nel caso dei tesserini di riconoscimento o per la formazione)
- relativi a comportamenti illeciti o fraudolenti (nel caso di segnalazioni di violazioni delle norme di legge)

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.7: Sistema di gestione della protezione del trattamento di dati

Descrizione (ovvero a riguardo di):

Documenti vari necessari al corretto adempimento delle misure di protezione, come previsto anche da norme di Legge.

Gli scopi del trattamento sono:

- Adempimento di un obbligo legale al quale è soggetto l'ente

I dati personali trattati sono:

- personali

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori
- fornitori
- terzi identificati e identificabili (nell'esercizio dei diritti degli interessati)

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.8: Sistema di gestione di prevenzione dei reati presupposto di cui al D.Lgs. 231/2001

Descrizione (ovvero a riguardo di):

Documenti vari relativi al modello di organizzazione, gestione e controllo per la prevenzione dei reati presupposto alla responsabilità amministrativa delle persone giuridiche.

Gli scopi del trattamento sono:

- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso
- accertamento, esercizio o difesa di un diritto in sede giudiziaria o ogniqualvolta le autorità esercitino le loro funzioni giurisdizionali
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- personali economici
- relativi a comportamenti illeciti o fraudolenti

L**e categorie di persone interessate sono:**

- soggetto stesso
- lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.9: Sistema informatico e di telecomunicazioni

Descrizione (ovvero a riguardo di):

Informazioni necessarie per garantire il funzionamento dell'insieme di postazioni informatiche (computer fissi, portatili, palmari, ecc.), stampanti, attrezzature di rete (switch, router, access point, firewall, ecc.) e server, atto al trattamento dei dati sia dal punto di vista software che hardware; in particolare per quanto attiene ai sistemi di autenticazione ed autorizzazione.

Mittente, destinatari, contenuto delle e-mail

Indirizzi degli host coinvolti, dati trasmessi, ecc. compresi indirizzi e contenuti delle pagine web visitate, contenuti delle sessioni di messaggerie

Gestione delle chiamate in entrata e in uscita gestito per fini amministrativi e commerciali.

Gli scopi del trattamento sono:

- Esigenze di natura organizzativa e produttiva
- Sicurezza e tutela del patrimonio (dell'ente, di terzi e delle persone) (cybersecurity)

I dati personali trattati sono:

- personali
- pseudonimi (quasianonimi) (nel caso dei tracciati dei log dei servizi tecnici)

L**e categorie di persone interessate sono:**

- soggetto stesso
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Servizio Firewall
- Servizio Software (antivirus)

Trattamento n.10: Sito web e newsletter

Descrizione (ovvero a riguardo di):

Dati tecnici indispensabili; statistiche di navigazione; dati per l'accesso all'area riservata; richieste di contatti; ecc.

Moduli di acquisizione dati personali, salvati sul db del sito ed inviati via mail alle funzioni preposte

Modulo per l'invio di comunicazioni semiautomatizzate (Newsletter) anche per scopi promozionali.

Gli scopi del trattamento sono:

- Attività commerciale
- Esigenze di natura organizzativa e produttiva
- Invio di informazioni ovvero contatto commerciale, promozionale e marketing
- Offerta di beni o prestazione di servizi agli interessati

I dati personali trattati sono:

- personali
- anonimi
- pseudonimi (quasianonimi) (tracciati dei log di navigazione e/o accesso alle pagine)

L**e categorie di persone interessate sono:**

- utenti
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Servizio Applicazione web (http://sviluppoinvestimentiterritorio.it/)

Il Preposto, in quanto persona autorizzata al trattamento

♦ Può trattare i dati personali contenuti nei documenti affidati nello svolgimento della sua attività nonché quelli contenuti in archivi cartacei, informatici o comunque costituiti, anche mediante l'utilizzo di strumenti elettronici. L'incaricato deve usare la massima riservatezza e discrezione nella tenuta dei dati di cui sopra e la massima diligenza nella conseguente loro protezione.
♦ Ha facoltà di utilizzare gli asset tecnologici in dotazione (dispositivi elettronici come quelli di rete o servizi specifici ecc.) per lo svolgimento dei compiti assegnati e per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute dal Titolare o dal Responsabile scrivente e anche dal delegante.

Nella regolamentazione interna, parte integrante delle istruzioni e disposizioni a cui ogni persona autorizzata al trattamento deve conformarsi, è puntualmente individuato per ciascuna unità di appartenenza l'ambito del trattamento consentito.

Il Preposto conosce direttamente ed approfonditamente gli obblighi assunti in relazione al dettato della legge e di possiede i requisiti di esperienza, capacità ed affidabilità idonei a garantire che il trattamento dei dati personali sia effettuato nel pieno rispetto delle vigenti norme in materia di trattamento dei dati personali.

Il Preposto si impegna, nel minor tempo necessario, ad impartire alle persone autorizzate al trattamento dei dati sotto la sua supervisione, ogni ulteriore istruzione relativa alle operazioni di trattamento che sia necessaria e funzionale alla corretta esecuzione dell'incarico affidato.

Il Preposto si impegna infine: a vigilare sulla corretta e puntuale applicazione delle suddette istruzioni; ad attenersi ad ogni istruzione che sia impartita successivamente alla presente designazione per ottemperare alle disposizioni di legge applicabili in merito di trattamento di dati personali.

Il Preposto, nel limite delle proprie attribuzioni, deleghe e compiti, risponde di qualsiasi operazione di trattamento di dati personali condotta in violazione dei suddetti compiti o delle direttive impartite.

10.2.2 Ambito Titolare del trattamento

Con riferimento al Regolamento Generale sulla Protezione dei Dati, Reg.(UE) 2016/679 e in considerazione di quanto in esso prescritto circa gli adempimenti e le misure di sicurezza da adottare, il soggetto nell'ambito della propria attività lavorativa inquadrata nella categoria omogenea di soggetti autorizzati al trattamento , deve, tra le altre funzioni e compiti:

- aver provveduto e provvedere continuativamente a determinare le finalità e i mezzi del trattamento

- svolgere personalmente e sovrintendere alle operazioni di trattamento di seguito riportate così come definiti internamente nei REAT, con le eventuali limitazioni e/o specificazioni del caso.

Trattamento n.1: SVILUPPO INVESTIMENTI TERRITORIO SRL

Descrizione (ovvero a riguardo di):

.

Gli scopi del trattamento sono:

- Attività amministrativo – contabili (connesse allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale)
- Esecuzione di un contratto di cui l'interessato è parte e/o di misure precontrattuali adottate su richiesta dello stesso
- Attività commerciale

I dati personali trattati sono:

- personali
- personali economici

Il titolare, come le altre persone autorizzate al trattamento

3. Può trattare i dati personali contenuti nei documenti affidati nello svolgimento della sua attività nonché quelli contenuti in archivi cartacei, informatici o comunque costituiti, anche mediante l'utilizzo di strumenti elettronici. L'incaricato deve usare la massima riservatezza e discrezione nella tenuta dei dati di cui sopra e la massima diligenza nella conseguente loro protezione.
4. Ha facoltà di utilizzare gli asset tecnologici in dotazione (dispositivi elettronici come quelli di rete o servizi specifici ecc.) per lo svolgimento dei compiti assegnati e per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute .

Il titolare conosce direttamente ed approfonditamente gli obblighi assunti in relazione al dettato della legge e possiede i requisiti di esperienza, capacità ed affidabilità idonei a garantire che il trattamento dei dati personali sia effettuato nel pieno rispetto delle vigenti norme in materia di trattamento dei dati personali impegnandosi ad adottare tutte le misure necessarie per la riservatezza e la protezione dei dati.

Il titolare si impegna, nel minor tempo necessario, ad impartire alle persone autorizzate al trattamento dei dati sotto la sua supervisione, ogni ulteriore istruzione relativa alle operazioni di trattamento che sia necessaria e funzionale alla corretta esecuzione dell'incarico affidato.

Il titolare si impegna infine: a vigilare sulla corretta e puntuale applicazione delle suddette istruzioni; ad attenersi ad ogni istruzione per ottemperare alle disposizioni di legge applicabili in merito di trattamento di dati personali.

11 Ulteriori istruzioni

Con il termine “categorie particolari di dati”, il GDPR individua quei dati che devono essere sottoposti ad una tutela particolare quali: dati personali che rivelino l'origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Fatta tale premessa, con valore di ordine di servizio, tutti i soggetti che rientrano nel “Mansionario riferito ai trattamenti di dati personali svolti internamente”, di cui alla sezione 10, debbono in particolare osservare le seguenti disposizioni:

- ogni persona autorizzata al trattamento che abbia ricevuto credenziali di autenticazione per il trattamento dei dati personali, deve conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve rispettare i criteri di lunghezza e complessità previsti dalla regolamentazione interna e comunque: deve essere di almeno 8 caratteri ovvero pari al massimo consentito, se inferiore; non deve contenere riferimenti agevolmente riconducibili all’incaricato;
- ogni persona autorizzata al trattamento deve modificare la parola chiave al primo utilizzo e, successivamente, secondo la frequenza e le modalità stabilite dalla regolamentazione interna e comunque almeno ogni tre mesi in caso di trattamento di categorie particolari di dati o di dati relativi a condanne e reati;
- ogni persona autorizzata al trattamento non deve in nessun caso lasciare incustodito o accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali, ad esempio azionando i meccanismi che bloccano o sospendono una sessione di elaborazione (screen saver);
- ogni persona autorizzata al trattamento deve attenersi alle istruzioni impartite dal Titolare o dal Responsabile del trattamento, nello svolgimento delle proprie mansioni di trattamento dati;
- ogni persona autorizzata al trattamento deve accedere ai soli dati personali la cui conoscenza è strettamente necessaria allo svolgimento dei compiti assegnati;
- ogni persona autorizzata al trattamento deve controllare e custodire, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali;
- ogni persona autorizzata al trattamento a cui sono affidati, per lo svolgimento dei relativi compiti, atti e documenti contenenti categorie particolari di dati o dati relativi a condanne e reati, controlla e custodisce tali atti e documenti fino alla loro restituzione verificando che non accedano persone prive di autorizzazione;
- eventuali supporti di memorizzazione riutilizzabili contenenti categorie particolari di dati o dati relativi a condanne e reati, possono essere riutilizzati solo se i dati precedentemente contenuti non sono più in alcun modo recuperabili, altrimenti devono essere distrutti;

- per il trattamento di categorie particolari di dati o dati relativi a condanne e reati su supporto cartaceo, i documenti devono essere custoditi in contenitori chiusi a chiave;
- nel caso in cui si verificasse la necessità di accedere ad archivi per i quali non si dispone dell'autorizzazione, ogni incaricato deve richiedere preventivamente tale autorizzazione al Titolare o al Responsabile o alle persone da questi delegate a tal fine;
- ogni persona autorizzata al trattamento deve rispettare il divieto di diffusione e di comunicazione a soggetti non preventivamente autorizzati, dei dati personali di cui verrà a conoscenza nell'ambito dell'attività di trattamento, non solo in vigenza della presente nomina, ma anche per tutto il tempo successivo durante il quale sarà in vigore tale divieto, senza limiti temporali;
- ogni persona autorizzata al trattamento deve informare tempestivamente il Titolare o il Preposto o il Responsabile in caso di violazioni dei dati personali.

12 Categorie di destinatari riferite ai trattamenti di dati personali svolti esternamente

Le categorie omogenee di destinatari riferite ai trattamenti di dati personali svolti esternamente sono:

- Assicurazioni
- Assistenza programma informatico
- Assistenza sistema informatico
- Assistenza sistema rilevazione presenze
- Banche
- Commercialista ed elaborazione contabilità
- Compagnie telefoniche
- Connettività internet
- Consulente Privacy
- Consulente Responsabilità Amministrativa
- Consulente Sicurezza sul lavoro
- Consulente lavoro ed elaborazione paghe
- Medico competente
- Notaio
- Organismo di vigilanza
- Provider PEC
- Provider dominio internet
- Provider posta elettronica
- Sindaco Unico
- Studio legale
- Trasporti e spedizioni
- Webmaster

12.1 Categoria: Assicurazioni

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Destinatario

12.2 Categoria: Assistenza programma informatico

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente alla manutenzione e configurazione di postazioni e programmi

12.3 Categoria: Assistenza sistema informatico

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Autorizzato al trattamento

12.4 Categoria: Assistenza sistema rilevazione presenze

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione del rapporto di lavoro nei confronti dei propri lavoratori come Responsabile del trattamento; riferito alle seguenti specificazioni/limitazioni: limitatamente alla fornitura e gestione del sistema di rilevazione presenze

12.5 Categoria: Banche

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Destinatario

12.6 Categoria: Commercialista ed elaborazione contabilità

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Responsabile del trattamento

- Gestione acquisti e approvvigionamenti come Responsabile del trattamento

12.7 Categoria: Compagnie telefoniche

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente al traffico telefonico

12.8 Categoria: Connettività internet

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente al traffico dati internet

12.9 Categoria: Consulente Privacy

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della protezione del trattamento di dati come Responsabile del trattamento

12.10 Categoria: Consulente Responsabilità Amministrativa

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione di prevenzione dei reati presupposto di cui al D.Lgs. 231/2001 come Responsabile del trattamento

12.11 Categoria: Consulente Sicurezza sul lavoro

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della sicurezza sul lavoro come Responsabile del trattamento

12.12 Categoria: Consulente lavoro ed elaborazione paghe

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione del rapporto di lavoro nei confronti dei propri lavoratori come Responsabile del trattamento

12.13 Categoria: Medico competente

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della sicurezza sul lavoro come Responsabile del trattamento

12.14 Categoria: Notaio

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Responsabile del trattamento

12.15 Categoria: Organismo di vigilanza

Tale categoria è assegnata ai seguenti trattamenti:

- Adempimenti per antiriciclaggio come Autorizzato al trattamento

12.16 Categoria: Provider PEC

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente al traffico telematico per l'erogazione dei servizi di posta elettronica certificata

12.17 Categoria: Provider dominio internet

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente al traffico telematico per l'erogazione dei servizi relativi al dominio internet dell'ente

- Sito web e newsletter come Destinatario; riferito alle seguenti specificazioni/limitazioni: hosting del sito

12.18 Categoria: Provider posta elettronica

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Destinatario; riferito alle seguenti specificazioni/limitazioni: limitatamente al traffico telematico per l'erogazione dei servizi di posta elettronica

12.19 Categoria: Sindaco Unico

Tale categoria è assegnata ai seguenti trattamenti:

- Direzione come Autorizzato al trattamento

- Adempimenti per antiriciclaggio come Autorizzato al trattamento

- Gestione amministrativo-contabile come Destinatario

12.20 Categoria: Studio legale

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Responsabile del trattamento; riferito alle seguenti specificazioni/limitazioni: limitatamente alla gestione di solleciti o recupero crediti di effetti scaduti

12.21 Categoria: Trasporti e spedizioni

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione attività di segreteria generale come Destinatario

12.22 Categoria: Webmaster

Tale categoria è assegnata ai seguenti trattamenti:

- Sito web e newsletter come Responsabile del trattamento