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

INSIT INDUSTRIA SPA

Identificativo nazionale (C.F.): 00937240042

Stato delle revisioni

Anno	Data	Descrizione
2024	12/11/2024	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

Torino, 12/11/24

Firma

SIG.RA DEBENEDETTI ANNA

Pagina intenzionalmente vuota

Sommario

1 Campo di applicazione 7
2 Riferimenti normativi 8
3 Definizioni 9
4 Obiettivi del sistema 14
5 Struttura del Sistema 15
6 Politica adottata 16
6.1 Principio di responsabilizzazione - Accountability 16
6.2 Privacy by Design e Privacy by Default 16
6.3 Principali adempimenti per il trattamento dei dati personali 16
6.3.1 Obbligo dell'informativa 16
6.3.2 Obbligo del consenso preventivo 17
6.3.3 Legittimo interesse nel trattare i dati 18
6.3.4 Registro delle attività di trattamento 22
6.3.5 Durata di conservazione dei dati 23
6.3.6 Valutazione d'impatto sulla protezione dei dati (DPIA) 23
6.3.7 Violazioni di dati personali (Data Breach) 25
6.3.8 Diritti degli interessati e gestione delle richieste 26
6.3.9 Trasferimenti di dati verso paesi extra-europei o organismi internazionali 29
6.3.10 Accordi, designazioni ed autorizzazioni 31
6.3.11 Diffusione del Modello organizzativo 31
6.3.12 Riesame ed aggiornamento 31
6.3.13 Codici di condotta 32
6.3.14 Meccanismi di certificazione 32
6.3.15 Regole deontologiche 33
6.4 Misure di sicurezza 34
6.4.1 Elenco delle sedi e dei locali 34
6.4.2 Registro degli asset di trattamento dati 34
6.4.3 Regolamento informatico 34
7 Ruoli, funzioni, poteri, compiti 36
7.1 Titolare del trattamento (TT) 36
7.1.1 Contitolarità 37
7.2 Responsabile del trattamento (RT) 37
7.2.1 Quando INSIT INDUSTRIA SPA è un Responsabile del trattamento per conto di altri 38

7.2.2 Scelta e designazione di un Responsabile del trattamento da parte di INSIT INDUSTRIA SPA 39
7.3 Autorizzato al trattamento (AT) ... 39
7.3.1 Nomina dell'Autorizzato al trattamento ... 40
7.4 Delega di funzioni ... 40
7.5 Preposto al trattamento (PT) ... 40
7.5.1 Nomina del Preposto al trattamento ... 41
7.6 Data Protection Officer (DPO) ... 41
7.6.1 Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali ... 42
7.6.2 Risorse necessarie ... 43
7.6.3 Indipendenza ... 43
7.6.4 Nomina del Data Protection Officer ... 44
7.6.5 Compiti del DPO ... 45
7.7 Rappresentante delegato del Titolare del trattamento o del Responsabile del trattamento ... 47
7.7.1 Preposto alla sicurezza del trattamento (PST) ... 47
7.8 Soggetti che si occupano di strumenti elettronici di supporto al trattamento dei dati ... 49
7.8.1 Amministratore di sistema (ADS) ... 49
7.8.2 Incaricato della gestione e della manutenzione degli strumenti elettronici (IGSE) ... 53
7.8.3 Autorizzato della custodia delle copie delle credenziali (ICCC) ... 53
7.8.4 Autorizzato delle copie di sicurezza delle banche dati (ICSBD) ... 54
7.8.5 Autorizzati della manutenzione o assistenza su particolari strumenti o programmi elettronici, senza qualifica di Amministratori di sistema (IMTZ) ... 55
7.9 Soggetti che potrebbero accidentalmente trattare dati ... 55
7.9.1 Addetto al controllo dei locali (ACL) ... 55
7.9.2 Addetti alla sorveglianza e vigilanza (ASV) ... 56
7.9.3 Addetti alle pulizie e manutenzioni ordinarie (APLZ) ... 57
8 Organigramma ... 59
9 Documentazione del sistema ... 60
9.1 Registri estesi delle attività di trattamento (REAT) ... 60
9.2 Procedure ed istruzioni operative ... 61
9.3 Report sull'adozione del GDPR ... 61
9.4 Accordi, incarichi e designazioni ... 62
9.5 Ulteriori evidenze documentali ... 62
10 Mansionario riferito ai trattamenti di dati personali svolti internamente ... 63
10.1 Categoria: CAPISQUADRA ... 63
10.1.1 Ambito Autorizzato al trattamento ... 63
10.2 Categoria: DIRIGENTI ... 67

10.2.1 Ambito Autorizzato al trattamento 67
10.3 Categoria: FIDUCIARIO PER WHISTLEBLOWING 70
10.3.1 Ambito Autorizzato al trattamento 70
10.4 Categoria: GENERAL MANAGER 71
10.4.1 Ambito Autorizzato al trattamento 71
10.5 Categoria: IMPIEGATI ACQUISTI 76
10.5.1 Ambito Autorizzato al trattamento 76
10.6 Categoria: IMPIEGATI AMMINISTRATIVI 79
10.6.1 Ambito Autorizzato al trattamento 79
10.7 Categoria: IMPIEGATI COMMERCIALI 82
10.7.1 Ambito Autorizzato al trattamento 82
10.8 Categoria: IMPIEGATI HR 86
10.8.1 Ambito Autorizzato al trattamento 86
10.9 Categoria: IMPIEGATI LOGISTICA 89
10.9.1 Ambito Autorizzato al trattamento 89
10.10 Categoria: IMPIEGATI TECNICI 92
10.10.1 Ambito Autorizzato al trattamento 92
10.11 Categoria: OPERAI 95
10.11.1 Ambito Autorizzato al trattamento 95
10.12 Categoria: OPERAI INTERINALI 98
10.12.1 Ambito Autorizzato al trattamento 98
10.13 Categoria: PERSONALE AUTORIZZATO ALL'UTILIZZO, TRASMISSIONE E DIFFUSIONE DI IMMAGINI E VIDEO 101
10.13.1 Ambito Autorizzato al trattamento 101
10.14 Categoria: RESPONSABILE IT 102
10.14.1 Ambito Autorizzato al trattamento 102
10.15 Categoria: RSPP 104
10.15.1 Ambito Autorizzato al trattamento 104
10.16 Categoria: RSU 105
10.16.1 Ambito Autorizzato al trattamento 105
10.17 Categoria: TITOLARE 107
10.17.1 Ambito Titolare del trattamento 107
10.17.2 Ambito Responsabile del trattamento 119
10.18 Ulteriori istruzioni per gli Autorizzati 119
11 Categorie di destinatari riferite ai trattamenti di dati personali svolti esternamente 121
11.1 Categoria: AGENZIE INTERINALI 122
11.2 Categoria: ASSISTENZA PER LO SMALTIMENTO RIFIUTI 122

11.3 Categoria: Assicurazioni 122
11.4 Categoria: Assistenza programma informatico 122
11.5 Categoria: Assistenza sistema informatico 122
11.6 Categoria: Banche 122
11.7 Categoria: COLLEGIO DEI REVISORI / SINDACI 122
11.8 Categoria: Commercialista ed elaborazione contabilità 123
11.9 Categoria: Compagnie telefoniche 123
11.10 Categoria: Connettività internet 123
11.11 Categoria: Consulente Privacy 123
11.12 Categoria: Consulente Sicurezza sul lavoro 123
11.13 Categoria: Consulente lavoro ed elaborazione paghe 123
11.14 Categoria: Consulente per la qualità 123
11.15 Categoria: ELABORAZIONE MODELLI INTRASTAT 124
11.16 Categoria: FORNITORE INSTALLAZIONE VIDEOSORVEGLIANZA 124
11.17 Categoria: FORNITORE PIATTAFORMA PER WHISTLEBLOWING 124
11.18 Categoria: FORNITORE SERVER 124
11.19 Categoria: GESTORE DELLA STRUMENTAZIONE ELETTRONICA 124
11.20 Categoria: Medico competente 124
11.21 Categoria: ORGANISMO DI VIGILANZA 124
11.22 Categoria: PORTALE COMMITTENTE 125
11.23 Categoria: Provider PEC 125
11.24 Categoria: Provider dominio internet 125
11.25 Categoria: Provider posta elettronica 125
11.26 Categoria: Studio legale 125
11.27 Categoria: Trasporti e spedizioni 125
11.28 Categoria: Webmaster 126

1 Campo di applicazione

Il Modello organizzativo per la protezione dei dati personali, quale parte integrante de 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 particolari (precedentemente noti come sensibili) e giudiziari.

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

L'ambito di applicabilità del Sistema ricomprende tutti i processi aziendali e di supporto che coinvolgono dati, informazioni e asset ad essi associati, quali applicazioni, sistemi di elaborazione, strumenti di storage, risorse umane e materiali, ambiente fisico e organizzazione. Pertanto, il presente documento riguarda tutti gli aspetti del trattamento di dati e informazioni, gestite sia attraverso supporti informatici sia manualmente. 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 INSIT INDUSTRIA SPA, ciascuno per quanto di propria competenza e spettanza. Quindi, tutti i soggetti (incaricati e non) che operano nell'ambito dell'organizzazione di INSIT INDUSTRIA SPA, 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 INSIT INDUSTRIA SPA, ed utilizzino le strutture messe a disposizione sono tenuti al rispetto scrupoloso del Sistema, nell'ambito delle proprie attività.

La continua evoluzione del contesto economico, normativo e tecnologico implica che le linee guida contenute in questo documento debbano essere periodicamente riesaminate per assicurare il mantenimento della loro adeguatezza.

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 (di qui in avanti anche brevemente “Regolamento” o “GDPR”)
- Norma nazionale – D.Lgs. 196/2003 integrato con le modifiche introdotte dal D.Lgs. 101/2018 (di qui in avanti anche brevemente “Codice privacy”)
- Provvedimenti dell’autorità di controllo nazionale, Garante per la protezione dei dati personali (d’innanzi, per brevità, “il Garante”)

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”
- Linee guida internazionali dell’European Data Protection Board - EDPB (Comitato Europeo per la Protezione dei Dati) e del Article 29 Working Party – WP29 (Gruppo di lavoro articolo 29)

3 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'**organizzazione** 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** 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.

4 Obiettivi del sistema

Gli scopi del Sistema sono:

- proteggere le informazioni e i dati personali da una ampia serie di minacce,
- garantire la conformità agli obblighi normativi in merito al trattamento dei dati e delle informazioni
- dare dimostrazione mediante evidenze della conformità agli obblighi normativi e delle misure di protezione,
- garantire il regolare ed efficiente svolgimento delle attività di INSIT INDUSTRIA SPA,
- rispettare i diritti e le libertà fondamentali delle persone relativamente al trattamento dei loro dati personali,
- ridurre gli eventuali danni sia alle persone interessate dai trattamenti, sia all'organizzazione.

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, aspirando ad:

- Aumentare la consapevolezza e accrescere il livello interno di conoscenza delle problematiche in cui si potrebbe quotidianamente incorrere durante le operazioni di trattamento di dati personali ordinarie e straordinarie;
- Aumentare l'efficienza e l'efficienza, ottimizzando le procedure interne di trattamento e controllo e le risorse disponibili.

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 INSIT INDUSTRIA SPA. 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.

5 Struttura del Sistema

INSIT INDUSTRIA SPA 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 possono 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 INSIT INDUSTRIA SPA 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 Politiche/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.

6 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 Regolamento art.5 com. 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.

6.1 Principio di responsabilizzazione - Accountability

Il Regolamento pone la "responsabilizzazione" (accountability nell'accezione inglese) quale principio fondamentale della normativa, respingendo le precedenti norme di concezione prettamente prescrittive. Così facendo affida al Titolare del trattamento l'onere di dimostrare la conformità normativa in materia di protezione dei dati personali, attraverso il rispetto dei principi di liceità e trasparenza e con l'adozione di misure organizzative e tecnologiche volte a garantire un livello adeguato di protezione.

6.2 Privacy by Design e Privacy by Default

Il Titolare del trattamento è tenuto a:

- considerare ("privacy by design") fin dalle fasi di progettazione, implementazione e configurazione di tutti i processi, i servizi aziendali, le attività e le tecnologie utilizzate per le operazioni di trattamento, gli aspetti in materia di protezione dei dati personali, in particolare le garanzie indispensabili per assicurare la conformità alla normativa e tutelare i diritti degli interessati, tra cui la custodia e il controllo; e
- trattare di default ("privacy by default") solamente quei dati personali che siano necessari al perseguimento delle finalità del trattamento, in osservanza del principio di minimizzazione dei dati.

6.3 Principali adempimenti per il trattamento dei dati personali

6.3.1 Obbligo dell'informativa

Un imprescindibile obbligo in capo al Titolare del trattamento è quello del rilascio agli interessati dell'informativa disciplinata dall'artt. 13-14 del Regolamento (UE) n. 2016/679, al fine di assicurare un'informazione chiara e completa, dunque adeguata, relativamente al trattamento dei loro dati, nonché un eventuale consenso al medesimo che sia effettivamente consapevole.

L'informativa deve essere data all'Interessato (cioè colui al quale i dati personali si riferiscono), sia quando i dati personali siano raccolti direttamente presso quest'ultimo, sia quando i dati dell'Interessato siano raccolti presso soggetti terzi.

L'informativa può essere orale o scritta, tenuto conto del fatto che il Titolare deve essere in grado di dare evidenza di averla fornita. Inoltre, l'informativa deve avere forma concisa, trasparente, intellegibile per l'interessato e facilmente accessibile, nonché avere un linguaggio chiaro e semplice. In particolare, l'informativa deve prevedere almeno i seguenti elementi:

- Identità e dati di contatto del Titolare del trattamento e del Data Protection Officer (DPO).;
- Finalità e la base giuridica del trattamento;
- Eventuali destinatari o categorie dei destinatari dei dati personali;
- Se i dati personali vengono trasferiti in Paesi terzi e in caso affermativo, attraverso quali garanzie;
- Periodo di conservazione dei dati o i criteri per determinarlo;
- Utilizzo di processi decisionali automatizzati;
- Possibilità per l'interessato di esercitare i propri diritti, ivi incluso il diritto di proporre reclamo ad un'autorità di controllo;
- Eventuale trattamento per una finalità diversa da quella per cui sono stati raccolti i dati.

Il testo delle informative è soggetto a revisione periodica; i testi sono storicizzati mediante un riferimento temporale alla data di revisione (es. "informativa aggiornata il gg/mm/aaaa").

6.3.1.1 Informativa laddove i dati non sono raccolti presso l'interessato

Qualora i dati non siano stati ottenuti presso l'interessato, coerentemente con la normativa vigente, al soggetto interessato vengono fornite alcune informazioni, tra cui l'identità e i dati di contatto del Titolare del trattamento e del DPO (e, ove applicabile, del rappresentante sul territorio), nonché le categorie di dati personali oggetto del trattamento, il periodo di conservazione dei dati personali o i criteri utilizzati per determinare tale periodo. L'interessato va, inoltre, informato della fonte da cui hanno origine i dati personali e se si tratta di dati provenienti da fonti accessibili al pubblico.

L'informativa deve essere fornita entro un mese dalla raccolta, oppure al momento della comunicazione dei dati.

In caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro, l'informativa ed il consenso al trattamento non sono dovuti. Al momento del primo contatto successivo all'invio del curriculum, il Titolare fornirà all'interessato, anche oralmente, una opportuna informativa ai sensi del Regolamento.

6.3.2 Obbligo del consenso preventivo

Ove la base giuridica del trattamento svolto dal soggetto scrivente in qualità di Titolare è il consenso, allora si deve acquisire un consenso specifico per ciascuna distinta finalità.

In particolare, il trattamento può non fondarsi sul consenso dell'interessato quando il trattamento medesimo:

- È necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- È necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- È basato sul legittimo interesse del Titolare del trattamento o di terzi purché siano bilanciati i diritti tra il Titolare e l'interessato (si veda il relativo paragrafo "Legittimo interesse nel trattare i dati").

Il consenso è validamente prestato solo nei casi in cui:

- È espresso liberamente, preventivamente e specificamente in riferimento ad ogni singolo trattamento chiaramente individuato.

Il soggetto giuridico scrivente prevede che:

- sia preventivamente resa l'informativa all'interessato, anche mediante la messa a disposizione dell'opportuna documentazione, consultabile a cura dell'interessato;
- il consenso sia preferibilmente fornito per iscritto o, in alternativa, sia comunque documentato mediante una registrazione (cioè annotando e conservando i riferimenti relativi all'interessato alla data, possibilmente con l'ora, il luogo di ricevimento, l'oggetto delle attività/servizi per i quali viene richiesto e l'indicazione della persona autorizzata che lo riceve; l'annotazione può avvenire ad es. in calce o in allegato alla copia dell'informativa o su una base dati digitale);
- se il consenso è espresso tramite App/Sito Web, ad esempio tramite apposizione di un flag in segno di autorizzazione al trattamento, prima dell'invio dei dati, raccolti mediante web form; oppure attraverso un comportamento chiaramente concludente da parte dell'interessato che insieme ai dati manifesta una propria specifica richiesta; è opportuno, soprattutto dove i dati sono memorizzati in archivi strutturati che rimanga un'evidenza dell'operazione con riferimenti all'utente, alla data/ora tramite la registrazione su di un supporto tecnico che non consenta modifiche rispetto a quanto espresso/visualizzato dall'interessato;
- il consenso sia fornito esclusivamente per iscritto o in modalità equivalenti in caso di dati particolari;

La modulistica che recepisce la manifestazione del consenso deve essere sempre conservata dalla funzione o unità organizzativa responsabile dello specifico trattamento, possibilmente insieme al testo dell'informativa (ad esempio, con i contratti, per i clienti, e nelle cartelle personali, per i dipendenti).

L'interessato può in qualsiasi momento revocare il consenso in precedenza manifestato, così come può in qualsiasi momento manifestare il proprio consenso in precedenza negato.

6.3.3 Legittimo interesse nel trattare i dati

Un trattamento di dati personali può svolgersi in base al legittimo interesse di terzi o del soggetto giuridico scrivente, in qualità di Titolare, (e quindi in assenza di consenso, obblighi normativi e contrattuali) quando è positivo l'esito del giudizio di bilanciamento (sulla base del test comparativo o balancing test proposto dal Working Party 29) tra i diritti delle parti coinvolte, che mira a verificare l'adeguatezza e legittimità del trattamento prendendo in considerazione:

- la natura dell'interesse dei terzi o del Titolare nonché
- i potenziali risvolti connessi al "mancato trattamento" e
- le possibili conseguenze che il trattamento da compiere potrebbe causare all'interessato,
- le ragionevoli aspettative dell'interessato al momento e nell'ambito della raccolta dei dati personali in base alla sua relazione con il Titolare,
- che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e,
- se l'interessato è un minore.

Nell'ambito del principio di accountability (artt. 5 e 24 del GDPR), spetta al soggetto giuridico scrivente il compito di effettuare e documentare il bilanciamento di interessi alla base del riconoscimento del legittimo interesse (che non è quindi più demandato al Garante[1]), che deve fornire motivazioni adeguate per le proprie scelte discrezionali.

Il balancing test è un obbligo in capo al Titolare con il duplice compito di:

- permettere di valutare la legittimità del trattamento che intende effettuare,
- dimostrare la conformità del trattamento con la norma applicabile.

[1] Si noti che prima del GDPR, fino al 24/05/2018, in Italia, tale valutazione di bilanciamento era prerogativa esclusiva del Garante.

Solo ove il balancing test dia un esito positivo, rilevando che il trattamento non lede i diritti vantati dall'interessato, il soggetto giuridico scrivente, quale Titolare del trattamento, può fare affidamento sul legittimo interesse quale base giuridica alternativa alle altre previste dal GDPR.

Il GDPR e la giurisprudenza del WP29, EDPB e del Garante italiano propongono alcuni esempi di "relazioni pertinenti e appropriate" nelle quali è possibile ipotizzare condizioni di legittimo interesse perseguito dal Titolare:

Norma di riferimento	Deduzione (diretta/per analogia)	Legittimo interesse (in sintesi)
GDPR, considerando 47	diretta	Trattare dati quando esista una relazione pertinente e appropriata tra l'interessato e il Titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del Titolare del trattamento
GDPR, considerando 47	diretta	Trattare dati personali strettamente necessari a fini di prevenzione delle frodi
GDPR, considerando 48	diretta	Trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti, fatti salvi i principi per il trasferimento verso un paese terzo extra-UE o extra-SEE
GDPR, considerando 49	diretta	Trattare dati personali relativi al traffico dati per garantire la sicurezza delle reti e dell'informazione (purché avvenga in misura strettamente necessaria e proporzionata)
GDPR, considerando 50	diretta	L'indicazione da parte del Titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica (purché soggetti un obbligo vincolante di segretezza)
GDPR, considerando 111	diretta	Acquisire dati da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un legittimo interesse per le finalità per cui il registro è reso disponibile (purché il trasferimento non riguardi la totalità dei dati personali o delle categorie di dati contenuti nel registro)
Garante, provvedimento generale in materia di videosorveglianza dell´8 aprile 2010 (doc. web n. 1712680)	diretta/ analogia	Trattare dati (immagini) per videosorveglianza (con registrazione fino a 72 ore e, se sul luogo di lavoro, previo accordo sindacale o autorizzazione della DTL)
GDPR, considerando 47	diretta	Trattare dati personali per finalità di marketing diretto
WP29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del	diretta	Svolgere attività di marketing basate su una profilazione c.d. "light" che non comporta un impatto rilevante sugli interessati cioè quando: a) il livello di dettaglio con cui viene definito un profilo non è invasivo: cioè le informazioni raccolte possono riferirsi a categorie ampie di individui e non sono mirate e granulari in modo da identificare, all'interno della più ampia categoria, il profilo di un singolo soggetto: la professione, il titolo di studio, la fascia di età sono informazioni di carattere generale in grado di coinvolgere un ampio numero di soggetti e per questo meno invasive;

Norma di riferimento	Deduzione (diretta/per analogia)	Legittimo interesse (in sintesi)
regolamento 2016/679, adottato il 3 ottobre2017		b) il profilo che emerge dalla raccolta delle informazioni raccolte non è completo per identificare univocamente un soggetto; c) l'impatto che l'attività di profilazione può avere sull'interessato non è rilevante per i diritti e le libertà fondamentali dell'individuo; d) le misure di sicurezza attuate assicurano la correttezza, l'accuratezza e prevengono la discriminazione nel processo di profilazione. NB. quando le condizioni di cui sopra non sono verificate il consenso rimane la base giuridica prediletta rispetto al trattamento per il perseguimento delle finalità di marketing e profilazione
Codice privacy, art. 130 co.4	diretta	Se il Titolare del trattamento utilizza (soft spam), a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni
Provvedimento del 4 ottobre 2011 Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro (doc. web n. 1850581)	diretta	Previo accordo sindacale o autorizzazione della DTL -garanzie previste dallo Statuto dei lavoratori (art. 4, comma 2, l. n. 300/1970) - trattare dati personali relativi all'ubicazione dei propri dipendenti per soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro
Linee-guida in materia di riconoscimento biometrico e firma grafometrica Allegato A al Provvedimento generale prescrittivo in tema di biometria del Garante del 12 novembre 2014	diretta	Previa adozione di tutte le misure e gli accorgimenti tecnici descritti nel provvedimento, è lecito trattare dati per: • autenticazione informatica biometrica; • controllo biometrico di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi; • uso delle impronte digitali o della topografia della mano a scopi facilitativi; • sottoscrizione di documenti informatici con firma grafometrica.
\WP217, Parere 6/2014 sul concetto di interesse legittimo del Responsabile del	analogia	Esercizio del diritto alla libertà di espressione e d'informazione, anche nei mezzi di comunicazione e di espressione artistica • con l'obiettivo di contribuire a una maggiore trasparenza e responsabilità, • in maniera accurata e proporzionata, adottando garanzie adeguate e, in senso più ampio, rispettando i diritti delle persone

Norma di riferimento	Deduzione (diretta/per analogia)	Legittimo interesse (in sintesi)
trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014		interessate, • tenuto conto o dell'interesse legittimo (un diritto fondamentale alla libertà di espressione o d'informazione), o dell'interesse del pubblico relativo alla trasparenza e alla responsabilità, o del fatto che la pubblicazione iniziale sia stata prevista dalla legge e che di conseguenza le persone si aspettassero che i loro dati sarebbero stati pubblicati
	analogia	Controllo del personale a fini di sicurezza o gestione • sia a fini di fatturazione che per la determinazione dei premi annuali • previa spiegazione trasparente ai dipendenti che hanno il diritto esplicito di esprimere il loro disaccordo con le conclusioni in termini sia di fatturazione che di pagamento del premio • tenuto conto che o non sembrano esistere mezzi meno invasivi per conseguire l'obiettivo in questione o l'impatto sui dipendenti è altresì limitato grazie alle garanzie e ai processi attuati o si potrebbe altresì sostenere che il trattamento per una o per entrambe le finalità è inoltre necessario all'esecuzione del contratto.
	diretta/ analogia	Trattare dati biometrici per sicurezza fisica, sicurezza informatica e sicurezza della rete • Quando sussiste un rischio elevato che sussisterebbe per la salute pubblica • Tenuto conto che o sono applicate garanzie adeguate, compreso il fatto che i dati biometrici sono conservati su i tesserini personali dei dipendenti e non in un sistema centralizzato o il motivo per cui i dati sono trattati è di interesse pubblico.
	analogia	Riutilizzo di dati disponibili al pubblico • a difesa della trasparenza e la responsabilità • tenuto conto che il trattamento si basi su informazioni pubbliche
	analogia	Sito web raccoglie, attraverso il proprio server, dati relativi ai visitatori del sito, purché subito resi anonimi e trasformati in dati statistici generali riguardanti le parti del sito web più consultate da visitatori provenienti da regioni geografiche differenti del paese e anche se i dati interessati riguardano soggetti vulnerabili Infatti: • il trattamento è di interesse pubblico e • sono poste in essere garanzie rigorose (i dati sono immediatamente anonimizzati e utilizzati solo per la creazione di statistiche)
Provvedimento n.163 del 12 settembre 2019 -	diretta/ analogia	Il trattamento dei dati personali da parte del gestore e dei partecipanti ad un sistema di informazione creditizia (SIC) secondo i termini e le condizioni stabilite nel Codice di condotta risulta lecito,

Norma di riferimento	Deduzione (diretta/per analogia)	Legittimo interesse (in sintesi)
Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti [doc. web n. 9141941]		senza consenso, ai sensi dell'art. 6 comma 1 lett. f) del Regolamento in quanto è necessario per il perseguimento di legittimi interessi dei partecipanti all'utilizzo del SIC per le finalità di cui al presente Codice di condotta. Costituiscono legittimi interessi: • la corretta misurazione del merito e del rischio creditizio, • la corretta valutazione dell'affidabilità e della puntualità dei pagamenti dell'interessato, • la prevenzione del rischio di frode, ivi inclusa la prevenzione del rischio del furto di identità. Per analogia il trattamento è legittimo se i dati sono raccolti e trattati dal soggetto giuridico scrivente quando è controparte contrattuale dell'interessato che risulta debitore o che potrebbe contrarre un debito o un'obbligazione di pagamento.

Pertanto, il legittimo interesse è invocato da INSIT INDUSTRIA SPA, quale Titolare del trattamento, per giustificare il trattamento dei dati personali connesso ad attività che non siano eccessivamente invasive per l'interessato ed in ragione di esigenze specifiche del Titolare, tenuto conto dei rapporti tra le parti nelle situazioni di cui alla tabella precedente per deduzione diretta o per analogia o, in assenza di correlazione, all'esito positivo del balancing test (per il bilanciamento degli interessi) di cui al Parere 6/2014 sul concetto di interesse legittimo del Responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE adottato il 9 aprile 2014 dal WP29, da conservarsi unitamente al registro delle attività di trattamento.

6.3.4 Registro delle attività di trattamento

INSIT INDUSTRIA SPA è tenuta a predisporre, ai sensi e in conformità all'art.30 del GDPR, un "registro dei trattamento" che identifichi le attività di trattamento di dati personali svolte in qualità di Titolare o di Responsabile del trattamento, al fine di monitorare i trattamenti dei dati personali svolti e per rendere più efficiente il reperimento di dati personali in caso di richieste da parte degli interessati e da parte dell'Autorità di Controllo.

Il Registro contiene l'elenco dei trattamenti gestiti, la descrizione del trattamento, la sua base legale, le sue finalità, i responsabili preposti e le strutture anche esterne che cooperano al trattamento, la natura dei dati trattati, una descrizione delle categorie di interessati, la struttura di riferimento, gli strumenti utilizzati e i tempi di conservazione dei dati, i trattamenti a rischio e le valutazioni di impatto sulla protezione dei dati realizzate, i trattamenti per i quali è richiesta la consultazione preliminare ai sensi dell'art.36 del GDPR all'Autorità Garante per la privacy. Inoltre dovrà contenere il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento, del Rappresentante delegato del Titolare del trattamento e del Responsabile della protezione dei dati (RPD o DPO) ; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative utilizzate.

Il registro dei trattamenti può avere forma scritta e/o elettronica, è revisionato con cadenza periodica e aggiornato ogniqualvolta un determinato evento possa determinare una modifica dello stesso (es. modifiche o aggiunte delle tipologie di dati personali trattati, definizione di nuove finalità di trattamento da prevedere nelle informative, modifiche contrattuali con terze parti, ecc.).

Il registro deve essere reso disponibile su richiesta all'Autorità di Controllo. Il registro è conservato a cura della funzione o unità organizzativa Responsabile del trattamento relativo al Sistema di gestione della protezione del trattamento dei dati (si veda il mansionario).

6.3.5 Durata di conservazione dei dati

Come recita il Considerando 39, il Titolare ha l'obbligo di "assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario" e che a tale fine "dovrebbe stabilire un termine per la cancellazione o per la verifica periodica".

Pertanto, l'individuazione della durata del trattamento deve essere ragionevole e contemperare adeguatamente le finalità di liceità, correttezza e trasparenza. In relazione alle diverse tipologie dei dati personali relativi alle persone fisiche alle finalità dei trattamenti, sono state identificati i seguenti casi:

- Per i trattamenti necessari per adempiere a un obbligo contrattuale o legale, il periodo di conservazione è determinato in funzione del relativo termine di prescrizione di cui all'art. 2946 e segg. del Codice civile;
- Per i trattamenti concernenti i dati relativi ai soggetti che esercitano funzioni di indirizzo, amministrazione, controllo e direzione, nonché ai soci del soggetto giuridico scrivente, il periodo di conservazione:
    - è fissato alla scadenza di un arco di tempo determinato oltre la cessazione dell'incarico, relativamente alla documentazione per la verifica dei requisiti;
    - non ha scadenza per i dati (anagrafici, titoli di studio, etc.) necessari ad esempio per esigenze storico/istituzionali (composizione storica, etc.).

Nei casi per i quali è Responsabile del trattamento, INSIT INDUSTRIA SPA procede, su scelta del titolare del trattamento, a cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e a cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

È stata adottata una specifica procedura "*Procedura per la distruzione e smaltimento di documenti cartacei contenenti dati personali*" presente all'interno del dossier "*Procedure*" per la distruzione dei dati al termine del periodo di conservazione.

6.3.6 Valutazione d'impatto sulla protezione dei dati (DPIA)

Per i trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone interessate viene svolta una valutazione di impatto (DPIA – Data Protection Impact Assessment) prima di dare inizio al trattamento o anche successivamente, qualora il rischio emergesse o venisse rilevato in un secondo tempo.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

La valutazione di impatto:

- è condotta ai sensi dell'articolo 35 del Regolamento e secondo le linee guida del EDPB o del Working Party 29;

- mira a descrivere il/i trattamento/i di dati per valutarne la necessità e la proporzionalità nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, allo scopo di approntare misure idonee per il corretto svolgimento dello stesso.
- è un processo inteso a garantire e dimostrare la conformità alla normativa vigente in tema di protezione dei dati personali che il Titolare è tenuto, nei casi previsti o quando ritenuto necessario, a svolgere.

In proposito, le linee guida del WP29 (doc. WP248rev.01 del 4 aprile 2017 modificato il 4 ottobre 2017) offrono alcuni chiarimenti, in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all'art. 35 del GDPR), chi debba condurla, in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori) e quando non sia richiesta.

La valutazione d'impatto sulla protezione dei dati è obbligatoria:

- Nei casi di cui all'art.35 co.3 del GDPR ovvero quando è svolta/o:
    a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
    b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del GDPR o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR; o
    c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
- Negli altri 12 casi di cui al provvedimento del Garante n. n. 467 dell'11 ottobre 2018 (doc. web. 4. 9058979), ai sensi dell'art.35 co.4 del GDPR
- Nelle ulteriori situazioni che presentano un rischio elevato per i diritti e le libertà delle persone interessate, anche sulla base delle linee guida vigenti.

La valutazione d'impatto sulla protezione dei dati, laddove previsto o ritenuto necessario, è adottata come strumento volto ad esprime chiaramente la responsabilizzazione (accountability) nei confronti dei trattamenti effettuati, al fine di

- rispettare i requisiti del Regolamento; ma anche
- dimostrare che sono state adottate misure appropriate per garantire il rispetto dello stesso.

6.3.6.1 Quando INSIT INDUSTRIA SPA è Titolare del trattamento

Qualora INSIT INDUSTRIA SPA sia il Titolare del trattamento dei dati personali per i casi e le situazioni in cui sussiste l'obbligo di DPIA, allora spetta a INSIT INDUSTRIA SPA, con la funzione competente degli adempimenti di protezione dei dati personali, coadiuvato dal DPO, se designato, condurre la valutazione, avvalendosi, se del caso, della collaborazione dei Responsabili del trattamento coinvolti.

Qualora il trattamento coinvolga oltre a INSIT INDUSTRIA SPA altri contitolari del trattamento, occorre definire precisamente le rispettive competenze. La valutazione d'impatto sulla protezione dei dati deve stabilire quale parte competa all'uno e all'altro per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati, senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate, etc.) o divulgare vulnerabilità.

In tutti i casi il Titolare giustifica e documenta sempre i motivi e i presupposti sui quali ci si è basati per non effettuare la valutazione d'impatto sulla protezione dei dati, nonché include/registra i punti di vista del DPO, ove designato.

Qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuarlo, allora, prima di procedere al trattamento, si deve consultare l'autorità di controllo ai sensi dell'art.36 del GDPR.

La DPIA non è intesa come un adempimento una tantum, bensì come processo soggetto a revisione periodica, se non continua.

6.3.6.2 Quando INSIT INDUSTRIA SPA è Responsabile del trattamento

Qualora INSIT INDUSTRIA SPA sia un Responsabile del trattamento dei dati personali per i casi e le situazioni in cui possa sussistere l'obbligo di DPIA, tenendo conto della natura del trattamento svolto per conto del Titolare del trattamento e delle informazioni in suo possesso che riguardano tale trattamento, allora INSIT INDUSTRIA SPA deve:

- informare il Titolare del trattamento sul rispetto dell'obbligo di cui agli articoli 35 e 36;
- assistere, coadiuvato dal DPO, se designato, il Titolare del trattamento, quando lo richiede, nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f) del GDPR).

6.3.7 Violazioni di dati personali (Data Breach)

Per Violazioni di dati personali (o Data Breach), ai sensi dell'art.33 del GDPR, si intende "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". Si intende dunque ogni violazione che incide su dati personali trattati sia con l'ausilio di strumenti digitali, sia senza.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Rientrano, dunque, nella definizione di Data Breach i seguenti eventi:

l'accesso o l'acquisizione dei dati personali da parte di terzi non autorizzati;

- il furto, la distruzione o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la distruzione o la perdita di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Sono esclusi dalla medesima i furti di documenti, supporti informatici, archivi, etc. non contenenti dati personali.

Qualsiasi incidente di sicurezza che possa riguardare una violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, sono annotate nel Registro delle Violazioni dei Dati (acronimo RVD).

La gestione della violazione dei dati avviene secondo le procedure interne di dettaglio tenuto conto di quanto segue.

In caso di violazione dei dati personali:

- Nei casi per i quali è Titolare del trattamento, INSIT INDUSTRIA SPA effettua la notifica della violazione al Garante per la protezione dei dati personali ai sensi dell'art. 33 del GDPR entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche INSIT INDUSTRIA SPA comunicare, quale Titolare del trattamento, a tutti gli interessati coinvolti l'avvenuta violazione con le indicazioni per ridurre i

rischi a loro carico. Qualora la notifica non sia effettuata entro 72 ore, devono essere espressi i motivi che hanno comportato il ritardo. È stata adottata una specifica procedura “Procedura per il monitoraggio e la gestione delle violazioni di dati (Data Breach)” presente all’interno del dossier “Procedure” per la qualificazione, valutazione e gestione della violazione dei dati.

- Nei casi per i quali è Responsabile del trattamento, INSIT INDUSTRIA SPA informa senza ingiustificato ritardo e, ove possibile e applicabile, entro i termini contrattuali pattuiti, il Titolare del trattamento in merito alla violazione e lo assiste, quando quest’ultimo lo richiede, nella gestione della violazione, fornendo tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f) del GDPR).

6.3.8 Diritti degli interessati e gestione delle richieste

Ogni persona fisica, in qualità di “Interessato”, ha facoltà di esercitare i propri diritti previsti dagli articoli da 15 a 22 del Regolamento.

Nei casi per i quali è Titolare del trattamento, INSIT INDUSTRIA SPA segue la seguente politica.

L'interessato può presentare un'istanza a INSIT INDUSTRIA SPA, senza particolari formalità (ad esempio, mediante posta elettronica, lettera raccomandata, ecc.), anche per tramite di un Responsabile del trattamento. L'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati.

La gestione delle richieste degli interessati avviene secondo le procedure interne di dettaglio tenuto conto di quanto segue.

Spetta a INSIT INDUSTRIA SPA:

- agevolare l’esercizio dei diritti da parte dell’interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea;
- fornire idoneo riscontro all'istanza:
  - senza ingiustificato ritardo, al più tardi entro un mese dal suo ricevimento;
  - tale termine può essere prorogato per ulteriori due mesi, qualora si renda necessario tenuto conto della complessità e del numero di richieste. In tal caso, il Titolare deve comunque darne comunicazione all'interessato entro 30 giorni dal ricevimento della richiesta;
- valutare la complessità del riscontro all’interessato;
- stabilire l’ammontare dell’eventuale contributo da chiedere all’interessato, soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice Privacy, ovvero se sono chieste più copie dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3 del GDPR); in quest’ultimo caso il Titolare deve tenere conto dei costi amministrativi sostenuti. Si tenga presente che l’esercizio dei diritti è, in linea di principio, gratuito per l’interessato.

Benché sia il solo INSIT INDUSTRIA SPA a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22), l’eventuale Responsabile del trattamento coinvolto è tenuto a:

- collaborare con INSIT INDUSTRIA SPA ai fini dell’esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e));
- informare INSIT INDUSTRIA SPA di eventuali richieste da parte degli interessati che sono pervenute al Responsabile del trattamento.

Il riscontro all'interessato di regola avviene in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1 del GDPR; si veda anche art. 15, paragrafo 3).

La risposta fornita all'interessato deve essere "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

INSIT INDUSTRIA SPA è tenuto a conservare per un periodo di tempo congruo le istanze pervenute dall'interessato, le comunicazioni, comprensive delle informazioni temporali, sulla tipologia, sul mezzo di comunicazione e sulle valutazioni in merito alla richiesta (es. soddisfacibilità, difficoltà, infondatezza, ripetitività, costi, misure da adottare, misure adottate, ecc.) e sulle azioni intraprese, comprese le comunicazioni di risposta all'interessato. È istituito il **Registro delle Richieste e delle Comunicazioni con l'Interessato** (con acronimo **RRCI**), su cui possono essere annotate anche in forma sintetica le informazioni principali circa le richieste degli interessati e le risposte fornite loro, sulla base delle eventuali procedure di dettaglio.

Inoltre, è stata adottata una specifica procedura "*Procedura per la gestione delle richieste degli interessati*" presente all'interno del dossier "*Procedure*" per la gestione delle richieste degli interessati.

Nei casi per i quali è Responsabile del trattamento, INSIT INDUSTRIA SPA informa senza ingiustificato ritardo e, ove possibile e applicabile, entro i termini contrattuali pattuiti, il Titolare del trattamento in merito alle richieste degli interessati e lo assiste, quando quest'ultimo lo richiede.

6.3.8.1 Diritto di accesso (Art. 15)

L'interessato ha diritto di ottenere da parte di INSIT INDUSTRIA SPA la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano. Fra le informazioni che il Titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi extra UE.

Il diritto di accesso comprende il diritto di ricevere una copia dei dati personali oggetto di trattamento. Il Titolare può consentire all'interessato di consultare direttamente, da remoto e in modo sicuro, i propri dati personali (si veda considerando 63 del GDPR).

6.3.8.2 Diritto di rettifica (Art. 16)

L'interessato ha, inoltre, il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Ai sensi dell'art.19 del GDPR, INSIT INDUSTRIA SPA deve comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche del trattamento effettuate salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. INSIT INDUSTRIA SPA è tenuto a comunicare all'interessato tali destinatari qualora l'interessato lo richieda.

6.3.8.3 Diritto di cancellazione (art.17)

L'interessato può richiedere la cancellazione dei dati personali che li riguardano senza ingiustificato ritardo se sussistono alcuni casi, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente, etc.

Non è richiesta la cancellazione dei dati qualora il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale oppure per motivi di interesse pubblico o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Ai sensi dell'art.19 del GDPR, INSIT INDUSTRIA SPA deve comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali richieste di cancellazione salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. INSIT INDUSTRIA SPA è tenuto a comunicare all'interessato tali destinatari qualora l'interessato lo richieda.

6.3.8.4 Diritto di limitazione del trattamento (art. 18)

Le attività di trattamento di dati personali sono limitate, su richiesta dell'interessato, in taluni casi, ad esempio se l'interessato contesta l'esattezza dei dati personali o si oppone al trattamento degli stessi, oppure se i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria e INSIT INDUSTRIA SPA non ha più bisogno di tali dati per il trattamento degli stessi, ecc.

È esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si oppone al loro trattamento ai sensi dell´art. 21 del Regolamento (in attesa della valutazione da parte del Titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, il Titolare adotta nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Ai sensi dell'art.19 del GDPR, il Titolare deve comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali richieste di limitazione del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. INSIT INDUSTRIA SPA è tenuto a comunicare all'interessato tali destinatari qualora l'interessato lo richieda.

6.3.8.5 Diritto alla portabilità dei dati (art. 20)

È diritto degli interessati di

- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti al Titolare
- far trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare cui li ha forniti, se tecnicamente possibile.

Sono portabili i dati personali che riguardano l'interessato o che sono stati forniti dall'interessato al Titolare.

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell´interessato o sulla base di un contratto stipulato con l´interessato (quindi non si applica, per esempio, ai dati il cui trattamento si fonda sull´interesse pubblico o sull´interesse legittimo del Titolare), e solo i dati che siano stati "forniti" dall´interessato al Titolare (si veda il considerando 68).

Poiché la trasmissione dei dati da un Titolare all'altro prevede che si utilizzino formati interoperabili, il Titolare adotta le misure necessarie a produrre i dati richiesti in un formato interoperabile tenendo conto delle indicazioni fornite nel considerando 68 e nelle linee-guida del Working Party 29.

6.3.8.6 Diritto di opposizione (art. 21)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del Regolamento, compresa la profilazione sulla base di tali disposizioni. INSIT INDUSTRIA SPA si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del Regolamento, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo che il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

6.3.8.7 Diritto a non essere sottoposti a processi decisionali automatizzati, compresa la profilazione (art. 22)

È diritto degli interessati richiedere di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o che incida in modo analogo significativamente sulla loro persona.

6.3.9 Trasferimenti di dati verso paesi extra-europei o organismi internazionali

In linea di principio, ai sensi del Capo V del Regolamento, sono vietati i flussi di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento al di fuori dell'Unione europea e dello spazio economico europeo (SEE, ossia tutta l'Unione Europea e Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale, fatti salvi i casi in cui intervengano specifiche garanzie che il Regolamento elenca in ordine gerarchico:

- adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (art. 45).;
- in assenza di decisioni di adeguatezza della Commissione, il trasferimento è consentito ove il Titolare (o il Responsabile del trattamento) fornisce garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46). Al riguardo, possono costituire garanzie adeguate:

  Senza autorizzazione da parte del Garante:
  - gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a));
  - le norme vincolanti d'impresa - BCR Binding Corporate Rules (art. 46, par. 2, lett. b) e art. 47);
  - le clausole contrattuali tipo – standard contractual clauses (art. 46, par. 2, lett. c e lett. d)), adottate dal Garante e approvate dalla Commissione Europea;
  - i codici di condotta (art. 46, par. 2, lett. e));
  - i meccanismi di certificazione (art. 46, par. 2, lett. f)).

  Previa autorizzazione specifica del Garante:
  - le clausole contrattuali ad hoc (art. 46, par. 3, lett. a));
  - gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b));
- in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (art. 49); è da ritenersi che il termine "deroga" includa di per sé una connotazione di eccezionalità rispetto al principio dell'adeguatezza e alle altre garanzie e che, pertanto, l'ambito di operatività delle suddette deroghe è soggetto ad un'interpretazione restrittiva. Le deroghe applicabili riguardano:
  - puntuale coinvolgimento dell'interessato (consenso, contratto);
  - contratto a favore dell'interessato;

- importanti motivi di interesse pubblico: deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del Titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente;
- accertare, esercitare o difendere un diritto in sede giudiziaria;
- tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- trasferimenti a partire da un registro pubblico ove sussista il cogente interesse legittimo del Titolare.

Sul sito del Garante (https://www.gpdp.it/web/guest/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale/trasferimento-dati-estero) a cui si rimanda per controllo e approfondimenti al fine dell'applicazione concreta caso per caso, sono riportati gli elenchi e il dettaglio applicativo in merito a:

- paesi per i quali sussiste una decisione di adeguatezza;
- strumenti giuridicamente vincolanti tra autorità pubbliche;
- clausole contrattuali tipo;
- BCR - norme vincolanti d'impresa.

Nel caso in cui il trasferimento dei dati fuori dell'Unione europea e dello spazio economico europeo sia necessario, INSIT INDUSTRIA SPA documenta tale necessità e verifica le garanzie applicabili, dandone evidenza nel Registro delle attività di trattamento e, ove applicabile, anche nell'informativa agli interessati.

Nei casi in cui INSIT INDUSTRIA SPA si avvalga di ulteriori soggetti, Responsabili del trattamento, verifica se le operazioni di trattamento che questi svolgono per suo conto, comportino flussi di dati verso Paesi Terzi o Organizzazioni internazionali: in tal caso, verifica la sussistenza dei requisiti di legittimità e, sulla base delle previsioni contrattuali, autorizza i responsabili del trattamento ad effettuare il trasferimento con istruzione documentata, ai sensi art.28 co.3 lett.a) GDPR.

Nei casi per i quali è Responsabile del trattamento, INSIT INDUSTRIA SPA informa il Titolare del trattamento di tale necessità e, prima di procedere con il trasferimento, ne attende l'autorizzazione con istruzione documentata. L'autorizzazione del Titolare non è necessaria quanto il trasferimento è previsto esplicitamente dal diritto dell'Unione o italiano: in tal caso, INSIT INDUSTRIA SPA specifica al Titolare del trattamento che si tratta di un obbligo giuridico, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

6.3.9.1 Fornitori USA di servizi cloud

Vista l'importanza dei servizi cloud, spesso erogati da soggetti stabiliti in USA, occorre sempre verificare che tali fornitori, se statunitensi, rientrino all'interno della cornice di legittimità[2], verificando la predisposizione di contratti basati sulle clausole contrattuali tipo (o standard contractual clauses - SCC) adottate con decisione n. 2010/87 relativa al trasferimento di dati personali a responsabili del trattamento stabiliti in Paesi terzi.

6.3.9.2 Requisiti dell'informativa in caso di trasferimenti di dati extra-europei

INSIT INDUSTRIA SPA deve informare gli interessati qualora vi sia intenzione di trasferire i dati personali verso un Paese extra-europeo o un'organizzazione internazionale e deve altresì indicare nell'informativa le condizioni in base alle quali avviene il trasferimento e il Paese verso quale avviene il trasferimento.

[2] La Corte di giustizia dell'Unione europea (CGUE) si è pronunciata il 16 luglio 2020 (c.d. "Sentenza Schrems II") in merito al regime di trasferimento dei dati tra l'Unione europea e gli Stati Uniti invalidando la decisione di adeguatezza del Privacy Shield, adottata nel 2016 dalla Commissione europea in seguito alla decadenza dell'accordo Safe Harbor.

6.3.10 Accordi, designazioni ed autorizzazioni

È vietato trattare dati personali se non si è istruiti in tal senso.

Ai sensi degli artt. da 26 a 29 e da 37 a 39 del GDPR e del all'art.2-quaterdecies del D.Lgs. 196/03 e s.m.i, nell'ambito del proprio assetto organizzativo, INSIT INDUSTRIA SPA[3]

- si accorda con gli altri contitolari del trattamento nei casi di contitolarità (art. 26 del GDPR);
- si accorda, mediante contratto o altro atto giuridico a norma, con ogni Titolare del trattamento (art. 28 del GDPR) per il cui conto effettua un trattamento di dati personali;
- si accorda, mediante contratto o altro atto giuridico a norma, con ogni Responsabile del trattamento (art. 28 del GDPR) a cui ricorre per effettuare un trattamento di dati personali in sua vece;
- designa il responsabile per la protezione dei dati (art. 37 del GDPR): obbligatoriamente, se ne ricorrono le condizioni; facoltativamente, altrimenti;
- designa le persone che, sotto alla propria diretta autorità, accedono e concorrono al trattamento dei dati personali, istruendole al riguardo (art. 29 del GDPR);
- designa le persone che, sotto alla propria diretta autorità, svolgono specifici compiti e funzioni connessi al trattamento di dati personali (art.2-quaterdecies del CP).

Ruoli, funzioni, poteri e compiti nonché le modalità ritenute opportune per formalizzare gli accordi o le designazioni di cui sopra sono descritti al paragrafo 7.

6.3.11 Diffusione del Modello organizzativo

Ai fini dell'efficacia del Sistema di gestione per la protezione dei dati e per la sicurezza delle informazioni è necessario garantire la corretta conoscenza delle indicazioni di condotta ivi contenute, con differente grado di approfondimento in relazione ai diversi ruoli e mansioni svolti dagli addetti autorizzati/responsabili nell'ambito delle attività di trattamento di dati personali.

In particolare, il Sistema di gestione è posto a conoscenza di tutte le risorse presenti in azienda, mettendo a loro disposizione la documentazione che lo costituisce e/o svolgendo specifiche attività di sensibilizzazione (es. informazione, formazione e addestramento): tutti gli addetti autorizzati devono prendere visione del Modello organizzativo, anche contestualmente – a seconda dei casi – agli atti di nomina o passaggio a nuove mansioni/funzioni, e assumono l'obbligo della relativa osservanza e contribuzione all'attuazione del Sistema di gestione.

6.3.12 Riesame ed aggiornamento

INSIT INDUSTRIA SPA, attraverso il personale incaricato, aggiorna ed eventualmente predispone una nuova versione del Modello Organizzativo contenente idonee informazioni riguardo al trattamento dei dati:

- con cadenza periodica e
- in occasione di:
    - modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché della libera circolazione di tali dati, o
    - in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o
    - a seguito di violazioni di dati significative o
    - quando i risultati della sorveglianza ne evidenzino la necessità.

A fini di riesame ed aggiornamento sono utili:

[3] Non si applica l'obbligo (art. 27 del GDPR) di designazione per iscritto di un rappresentante nell'Unione Europea, in quanto INSIT INDUSTRIA SPA è stabilito nell'Unione Europea e, pertanto, non si applica l'articolo 3, paragrafo 2, il del GDPR.

- mappatura delle modifiche intervenute a livello aziendale relativamente a: personale; modelli di business che coinvolgono i dati personali; procedure interne; strumenti e modalità di trattamento dei dati personali;
- analisi dell'impatto delle novità normative e giurisprudenziali in materia di protezione dei dati personali sulla realtà aziendale e sugli specifici trattamenti effettuati, e della conformità del Sistema di gestione per la protezione dei dati e per la sicurezza delle informazioni a tali aggiornamenti;
- verifica dei provvedimenti normativi e tecnici relativi a decisioni di adeguatezza, clausole contrattuali tipo, codici di condotta, meccanismi di certificazione, regole deontologiche, provvedimenti di carattere generale, linee guida e ogni altro disposizione attinente ed applicabile in generale al fine di valutarne l'adozione per il Sistema di gestione anche ai fini dell'applicazione diretta o analogica del legittimo interesse;
- verifica del rispetto dei provvedimenti specifici del Garante a cui è soggetta l'organizzazione;
- verifica delle misure tecniche e organizzative e degli eventuali incidenti di sicurezza e violazioni di dati subiti dall'azienda, per la predisposizione di misure correttive;
- analisi – in caso di provvedimenti sanzionatori comminati all'azienda – delle eventuali richieste di informazioni rivolte dall'Autorità Garante all'azienda e un esame dei verbali di ispezione, per una revisione sostanziale dei trattamenti dalla cui effettuazione è scaturita la sanzione;
- verifica della correttezza del Registro dei trattamenti e della documentazione di implementazione sulla base di quanto emerso ai punti precedenti;
- sessione formativa di aggiornamento rivolta al personale autorizzato;
- redazione di un Report finale sul mantenimento dello stato di compliance al GDPR.

6.3.13 Codici di condotta

Premesso che:

- Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta (Art. 40 del GDPR) destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.
- Qualsiasi soggetto (associazioni, organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento) può elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del Regolamento.
- Le associazioni e gli altri organismi che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente, che esprimerà un parere sulla conformità al Regolamento del progetto di codice, della modifica o della proroga ed approverà, se del caso, tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'art. 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

Si provvede periodicamente, in occasione del riesame ed aggiornamento, a verificare la disponibilità e l'opportunità di adesione di:

- Codici di condotta approvati dall'autorità di controllo sui siti https://www.gpdp.it/web/guest/codici-di-condotta.

6.3.14 Meccanismi di certificazione

Premesso che:

- Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione (Art. 42 del GDPR) della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti svolti.

Si provvede periodicamente, in occasione del riesame ed aggiornamento, a verificare la disponibilità e l'opportunità di adozione di:

- meccanismi di certificazione approvati da Garante e da Accredia (ente nazionale di certificazione) sul sito https://www.accredia.it/privacy

Tuttavia, ad oggi, le certificazioni rilasciate dagli organismi accreditati (https://www.accredia.it/certificazioni-volontarie) non sono ancora validate ai sensi del GDPR, ma sono riconosciute dal mercato come una garanzia e un atto di diligenza dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme del Regolamento. Non esiste pertanto alcuna "esimenza" giuridica rispetto alle possibili sanzioni e imputazioni di colpevolezza che possono derivare da illeciti come, per esempio, un Data Breach o la mancata liceità di un trattamento.

6.3.15 Regole deontologiche

Premesso che

- Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto;
- Il rispetto delle disposizioni contenute nelle regole deontologiche di cui sopra costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali,

si provvede periodicamente, in occasione del riesame ed aggiornamento, a verificare la presenza e l'applicabilità di:

- Regole deontologiche pubblicate ai sensi dell'art. 2-quater 4, del D.Lgs. 196/2003 e s.m.i. sul sito https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9069732 e nell'Allegato A del Codice Privacy sul sito https://www.gpdp.it/codice.

Allo stato attuale, le regole deontologiche vigenti riguardano:

- A.1 - "*Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica*" (G.U. del 4 gennaio 2019, n. 3);
- A.2 - "*Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria*" (G.U. del 15 gennaio 2019, n. 12).
- A.3 - "*Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica*" (G.U. del 15 gennaio 2019, n. 12);
- A.4 - "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale*" (G.U. del 14 gennaio 2019, n. 11);
- A.5 - "*Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*" (G.U. del 14 gennaio 2019, n. 11).

6.4 Misure di sicurezza

INSIT INDUSTRIA SPA è tenuto ad implementare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e volte a garantire il rispetto e i diritti e delle libertà degli interessati.

La scelta delle misure di sicurezza da implementare deve tenere in considerazione i rischi che derivano dalla possibilità di distruzione non autorizzata, perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, corruzione e fuoriuscita di dati personali trattati.

Sulla base del principio di Privacy by design, è necessario definire anticipatamente le misure di sicurezza, effettuando un'analisi preventiva da aggiornarsi periodicamente; sul base del principio di Privacy by default, i sistemi automatizzati di trattamento dei dati devono essere configurati conseguentemente alle misure definite.

Gli approfondimenti e le misure di tipo tecnico, generali o per ciascun sistema, possono essere descritte in uno o più regolamenti o in policy di sicurezza dedicate.

6.4.1 Elenco delle sedi e dei locali

INSIT INDUSTRIA SPA adotta e tiene aggiornato un “Elenco delle sedi e dei locali” su cui basare le valutazioni.

L’elenco riporta l’indirizzo completo delle sedi appartenenti alla scrivente organizzazione e presso le quali vengono trattati i dati. Suddivise per sede, sono indicate le aree in cui sono contenuti archivi cartacei, elettronici, magnetici, ottici, ecc. dei dati dell’organizzazione (cioè dossier, documenti, computer, server, copie dei dati su cassetta o cd, ecc.), o in cui si svolge una fase del trattamento e descritte le caratteristiche del locale.

6.4.2 Registro degli asset di trattamento dati

INSIT INDUSTRIA SPA adotta e tiene aggiornato un “Elenco degli asset di trattamento” dati su cui basare le valutazioni.

Al fine di mantenere aggiornato il modello organizzativo per la protezione dei dati e per la sicurezza informatica, sono predisposti all’interno del dossier “*Facsimili di Registrazione*”, i registri da compilare riguardo gli asset di trattamento utilizzati e implementati nel proprio sistema (specifiche sui computer, sui tablet/smartphone, modalità di backup, specifiche dei sistemi antivirus e firewall ecc.).

6.4.3 Regolamento informatico

INSIT INDUSTRIA SPA adotta e tiene aggiornato un regolamento interno sull’uso degli strumenti informatici utilizzati dal personale autorizzato, il cui scopo è quello di dettare le procedure per una corretta e adeguata gestione delle risorse informatiche e telematiche aziendale.

L'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, pertanto si ritiene utile adottare ulteriori regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti e per risponde, come previsto dal Provvedimento dell’Autorità Garante per la Privacy del 1° marzo 2007, anche all’esigenza di dare una corretta informativa su:

- uso dei dati automaticamente ed implicitamente “trattati” a causa dell’uso di elaboratori informatici, di apparati telefonici e di dispositivi mobili quali smartphone e tablet;
- norme per la limitazione della navigazione;

- norme per l'uso della posta elettronica e i sistemi di messaggistica;
- sistemi di log;
- controlli sull'uso dei dispositivi e sull'applicazione del regolamento.

7 Ruoli, funzioni, poteri, compiti

7.1 Titolare del trattamento (TT)

Si richiama la definizione di “Titolare del trattamento”, cioè “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”.

Nel caso il Titolare sia un soggetto giuridico non persona fisica, come per INSIT INDUSTRIA SPA, 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, a seconda dei casi e delle deleghe, le decisioni potrebbero essere assunte da un amministratore delegato o dall’amministratore unico, dall’intero consiglio di amministrazione, dal direttore generale, ove presente, o da altri dirigenti o da altre persone fisiche che abbiano il potere di rappresentare il soggetto giuridico mediante atto di attribuzione dei poteri, delega o procura. Pertanto, ai fini del GDPR, Titolare del trattamento è il soggetto giuridico. A fronte delle delibere assunte dall’alta direzione INSIT INDUSTRIA SPA, gli adempimenti previsti per il Titolare del trattamento sono attribuiti in capo a: SIG.RA DEBENEDETTI ANNA (Rappresentante delegato del Titolare del trattamento). 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;

- 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.

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)

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 anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- 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;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- 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;
- informare il Titolare ovvero il soggetto delegato quale Preposto alla sicurezza del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
- non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche;
- adotti tutte le misure richieste ai sensi dell'articolo 32;
- su scelta del Titolare del trattamento, cancella o restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati
- metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente elenco puntato e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

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;
- se persona fisica, compiere direttamente le operazioni di trattamento, come gli Autorizzati che operino sotto la sua diretta autorità.

7.2.1 Quando INSIT INDUSTRIA SPA è un Responsabile del trattamento per conto di altri

Nel caso il Responsabile del trattamento sia un soggetto giuridico non persona fisica, come per INSIT INDUSTRIA SPA , 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, a seconda dei casi e delle deleghe, le decisioni potrebbero essere assunte da un amministratore delegato o dall'amministratore unico, dall'intero consiglio di amministrazione, dal direttore generale, ove presente, o

da altri dirigenti o da altre persone fisiche che abbiano il potere di rappresentare il soggetto giuridico mediante atto di attribuzione dei poteri, delega o procura. Pertanto, ai fini del GDPR, Responsabile del trattamento è il soggetto giuridico. A fronte delle delibere assunte dall'alta direzione INSIT INDUSTRIA SPA, gli adempimenti previsti per il Responsabile del trattamento sono attribuiti in capo a: SIG.RA DEBENEDETTI ANNA (Rappresentante delegato del Responsabile del trattamento). I documenti, qualora necessari, che comprovano tale assunto devono essere conservati in luogo sicuro.

7.2.2 Scelta e designazione di un Responsabile del trattamento da parte di INSIT INDUSTRIA SPA

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

La designazione del Responsabile del trattamento avviene ai sensi dell'art.28 GDPR; in linea generale la designazione è a tempo determinato, salvo diversa specificazione; è correlata con gli altri contratti commerciali con il soggetto designato; 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. 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, nell'atto della nomina, rilascia una dichiarazione da cui risulti che adottata o si impegna ad adottare tempestivamente le misure idonee di sicurezza per il trattamento.

7.3 Autorizzato al trattamento (AT)

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

La designazione[4] è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Quindi, gli Autorizzati al trattamento dei dati ricevono idonee ed analitiche istruzioni, preferibilmente scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

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.

[4] 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.

- 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 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 di responsabili ed autorizzati, sussiste la facoltà 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 delegante 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, salvo questo non sia esplicitamente previsto nelle delega iniziale o specificamente autorizzato anche successivamente.

7.5 Preposto al trattamento (PT)

Per esigenze organizzative, possono essere designati preposti al trattamento (PT), anche mediante suddivisione di compiti, le persone diverse dai responsabili del trattamento che sono incardinate internamente a INSIT INDUSTRIA SPA.

Il Preposto è la persona fisica, individuata tra le persone autorizzate al trattamento, preposta al trattamento di dati. Il Preposto è designato dal soggetto giuridico scrivente 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, 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.

7.5.1 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)

INSIT INDUSTRIA SPA, in relazione all'attività svolta, deve[5], se ne ricorrono le condizioni necessarie, oppure, in alternativa, può[6] volontariamente, individuare, nominare e incaricare per iscritto, un Responsabile per la protezione dei dati ovvero Data Protection Officer (DPO).

[5] 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.

[6] 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.

Questa figura rappresenta un elemento importante 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[7].

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, INSIT INDUSTRIA SPA (sia come Titolare del trattamento, sia come responsabile del trattamento) assicura 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 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] 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.

7.6.2 Risorse necessarie

Ai sensi dell'articolo 38, paragrafo 2, del GDPR, INSIT INDUSTRIA SPA sostiene 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 tali 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 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. Resta fermo l'obbligo di comunicare il nominativo del DPO all'autorità di controllo, procedura fondamentale affinché il DPO funga da punto di contatto fra la scrivente organizzazione e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e).

INSIT INDUSTRIA SPA ha ritenuto di provvedere alla designazione del Data Protection Officer (DPO), quale Responsabile della protezione dei dati, con incarico a:

Denominazione: SPAZIOTTANTOTTO S.R.L., avente C.F./P.Iva: 08283280017

Soggetto individuato quale referente per il Titolare/Responsabile: MARTINI FABRIZIO

Data nomina: 30/11/2023

Comunicazione al garante: Si

Numero di protocollo della comunicazione: _____

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. 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.

7.6.5.6 Preposto al riscontro all'interessato (PRI)

Coadiuvato dal Titolare del trattamento, il DPO, risponde prontamente alle richieste degli interessati, in esecuzione di quanto disposto dagli artt. 7, 8, 9 e 10 del Codice Privacy e, comunque fornisce agli interessati tutte le informazioni prescritte dalla legge.

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

Al DPO, quale figura di collegamento con il Garante, sono affidate in tutto o in parte le seguenti responsabilità e compiti:

1. rappresentare INSIT INDUSTRIA SPA (quale Titolare e/o Responsabile del trattamento) 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 Rappresentante delegato del Titolare del trattamento o del Responsabile del trattamento

Il Rappresentante delegato del Titolare del trattamento o del Responsabile del trattamento (talvolta anche indicato come "Delegato Privacy") sulla base di quanto indicato ai §7.1 e §7.2.1 è il soggetto con facoltà di designazione, che si occupa, tra l'altro, di designare le persone che, sotto la diretta autorità di INSIT INDUSTRIA SPA, svolgono specifici compiti e funzioni connessi al trattamento di dati personali.

Il Rappresentante delegato del Titolare del trattamento o del Responsabile del trattamento è anche autorizzato a trattare i dati personali secondo il profilo di Preposto al trattamento di cui al §7.5 e sulla base di una dichiarazione scritta a propria firma anziché la nomina prevista al §7.5.1

Qualora il Rappresentante delegato del Titolare del trattamento o del Responsabile del trattamento non abbia ritenuto di assegnare nominativamente i seguenti ruoli, secondo i profili descritti nel prosieguo, ne assume tutte le responsabilità e funzioni.

7.7.1 Preposto alla sicurezza del trattamento (PST)

INSIT INDUSTRIA SPA, 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.

Il Preposto è la persona che sovrintende all'attività lavorativa e ne controlla la corretta esecuzione da parte dei lavoratori, garantendo l'attuazione delle direttive ricevute, esercitando un funzionale potere di iniziativa, in ragione delle competenze professionali e nei limiti dei poteri gerarchici che gli derivano dalla natura dell'incarico che gli è stato conferito.

Il Preposto alla sicurezza del trattamento è la persona fisica (designata anche mediante contratto con altra persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo) a cui sono affidate le seguenti responsabilità e compiti:

1. Redigere ed aggiornare ad ogni variazione la documentazione di cui gli adempimenti richiamanti al paragrafo "Politica adottata ".
2. Garantire che tutte le misure di sicurezza riguardanti i dati (personali e non) siano applicate.
3. 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.
4. Proporre se affidare il trattamento dei dati in tutto o in parte all'esterno dell'organizzazione, tenuto conto di eventuali limitazioni derivanti da accordi o incarichi con terze parti (ad es. nei casi di contitolarità o ove si intenda ricorrere ad un responsabile successivo – art.28 co.2 del GDPR).
5. Qualora il trattamento dei dati personali sia stato affidato in tutto o in parte all'esterno controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
6. Individuare e fornire istruzioni documentate ai Responsabili del trattamento ed agli Autorizzati per garantire la sicurezza del trattamento.

7. Nominare e incaricare per iscritto gli Autorizzati e, ove lo ritenesse opportuno, i Preposti a 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 automatizzato o effettuato con strumenti elettronici di elaborazione dei dati, provvede a:
   a) individuare, nominare e incaricare per iscritto, uno o più
      i. Amministratori di Sistema,
      ii. Incaricati della gestione e della manutenzione degli strumenti elettronici;
      iii. Autorizzati della custodia delle copie delle credenziali qualora vi sia più di un Autorizzato al trattamento;
      iv. Autorizzati delle copie di sicurezza delle banche dati, anche con il compito di custodire e conservare i supporti utilizzati per le copie dei dati;
   b) qualora il Preposto alla sicurezza del trattamento ritenga di non nominare una delle figure di cui sopra, ne assumerà tutte le responsabilità e funzioni;
   c) 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:
      i. redigere ed aggiornare ad ogni variazione l'elenco dei soggetti nominati quali Incaricati 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;
      ii. verificare, con cadenza almeno annuale, l'attività svolta dagli Incaricati 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;
      iii. 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;
      iv. 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.
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 INSIT INDUSTRIA SPA;
   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.

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.

7.8 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.

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 (designata mediante contratto con altra persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che sovrintende al buon funzionamento degli asset (service o device, fisici o virtuali) e relativi trattamenti.

L'Amministratore di sistema svolge le attività a lui affidate nel rispetto della normativa vigente in materia di sicurezza e protezione dei dati personali, delle istruzioni e direttive impartite dal Titolare del trattamento e/o dal responsabile del trattamento.

L'Amministratore di sistema accede esclusivamente ai dati personali ai quali è stato autorizzato ad accedere e tratta soltanto i dati personali necessari allo svolgimento delle attività, di cui all'incarico, per garantire il funzionamento dei sistemi affidategli (es. applicazioni, banche dati, sistemi software, elaboratori, strumenti elettronici, apparati di sicurezza, etc. da qui in avanti brevemente "**Sistemi informatici**")

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

- figure professionali finalizzate alla gestione e alla manutenzione di sistemi di elaborazione e/o di loro componenti (così come avviene generalmente in ambito informatico), di banche dati, di reti di telematiche, di sistemi software, di strumenti elettronici e di apparati di sicurezza.

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.

Pertanto, la designazione quale Amministratore di sistema deve essere individuale e deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve offrire anche sulla base delle ordinarie attività svolte e dei compiti assegnati, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza.

L'Amministratore di sistema deve dare pieno adempimento al Provvedimento del Garante del 27 novembre 2008 (pubblicato in G.U. n. 300 del 24/12/2008) come modificato ed integrato dal provvedimento del 25 giugno 2009 (pubblicato in G.U. n. 149 del 30/06/2009) recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"[8].

Compiti dell'Amministratore di sistema:

- Definire quali politiche adottare per la protezione dei Sistemi informatici contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
- Proteggere i Sistemi informatici dal rischio di intrusione (violazione del sistema da parte di "hackers").
- Installare e mantenere aggiornato il sistema di protezione contro i virus e i programmi pericolosi.
- Verificare il costante corretto funzionamento dei meccanismi di sicurezza, segnalando le eventuali violazioni, tentativi di violazione, anomalie di utilizzo o deficienze riscontrate.
- Informare nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali, sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti o situazioni critiche.
- Attivare le credenziali di autenticazione agli utenti del sistema informatico, su indicazione del Titolare del trattamento.
- Gestire e garantire la custodia non in chiaro, ove tecnicamente fattibile, delle credenziali per l'accesso ai dati degli utenti del sistema informatico.
- Istruire gli utenti del sistema sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
- Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'utente del sistema l'accesso ai dati personali.
- Revocare le credenziali per l'accesso ai dati degli Utenti del sistema nel caso di mancato utilizzo per oltre 6 (sei) mesi.
- Supportare gli utenti nella risoluzione di qualunque problematica o anomalia degli asset informatici utilizzati e nell'attuare, per i medesimi asset, le misure di sicurezza previste.

[8] 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 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.

- Gestire e sovrintendere la pianificazione, l'esecuzione, l'eventuale sostituzione, la custodia e il ripristino delle copie di sicurezza del sistema, secondo quanto dettagliato nella procedura interna di salvataggio dati.
- Sovrintendere al buon funzionamento dei Sistemi informatici nel loro complesso.
- Gestire le risorse ai fini della sicurezza informatica.
- Valutare se le risorse in dotazione sono sufficienti a garantire l'applicazione delle regole definite ed eventualmente proporre l'acquisizione di ulteriori risorse per migliorare i livelli di servizio, compresa la sicurezza dei dati.
- Descrivere le regole per la gestione dei profili di accesso ai Sistemi informatici.
- Configurare i sistemi informatici in ottemperanza alle regole di accesso ai dati, sulla base delle prescrizioni dei regolamenti interni alla struttura del Titolare del trattamento.
- Inserire e modificare i profili utente di sistema attribuendo e revocando le autorizzazioni sulla base delle relative esigenze di lavoro, su segnalazione del Titolare del trattamento e dei soggetti da questo delegati.
- Rilasciare e revocare le autorizzazioni di accesso ai Sistemi informatici.
- Configurare i sistemi per registrare gli accessi logici (autenticazione informatica) ai Sistemi informatici: le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate; devono essere conservate per un congruo periodo, non inferiore a sei mesi nel caso delle persone fisiche incaricate quali Amministratori di sistema; inoltre devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità.
- Verificare, con periodicità almeno annuale, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, con individuazione dell'ambito del trattamento consentito ai singoli utenti del sistema, conservandone le relative liste di evidenza;
- Verificare, in caso di condivisione del sistema tra più Titolari del trattamento, che le impostazioni del sistema garantiscano la separazione degli ambienti e dei profili.
- Informare nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.
- Informare nel caso di violazioni di dati, adottando tempestive contromisure e collaborando alle valutazioni ed azioni conseguenti.
- Fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dat personali, ivi compreso il profilo relativo alla sicurezza.

All'Amministratore di sistema, insieme agli altri eventuali Amministratori, spetta il compito di provvedere alla stesura ed all'aggiornamento del manuale di sicurezza dei Sistemi informatici, in cui sono dettagliati il livello dei servizi indicati per i sistemi affidati all'Amministratore e le relative procedure di sicurezza, al fine di mantenere o migliorare i livelli di servizio in base all'evoluzione della tecnica, allo stato dell'arte, dei rischi e delle minacce che incombono sui sistemi amministrati e di conseguenza sui dati e sui diritti degli interessati.

Inoltre, collabora con le altre persone individuate dal soggetto scrivente ad amministrare i Sistemi informatici per garantire la sicurezza complessiva.

L'Amministratore provvede ad informare in caso di variazioni ed aggiornamenti del manuale.

Compiti svolti fuori dai locali del Titolare e/o con mezzi propri

Per il trattamento in esterno dei dati personali, svolti fuori dai locali della scrivente organizzazione, si debbono osservare le seguenti disposizioni:

- nella struttura esterna, presso cui si effettui il trattamento dei dati, devono essere adottate idonee misure di sicurezza per garantire la riservatezza e l'integrità dei dati;

- durante una sessione di trattamento dei dati personali, lo strumento elettronico non deve essere lasciato incustodito e accessibile.

L' Amministratore di sistema ha 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.

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 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).

Spettano tipicamente all'Amministratore di sistema[9]: la gestione dei sistemi di autenticazione e di autorizzazione; la custodia delle componenti riservate delle credenziali di autenticazione; la realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati). 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. 29 del GDPR) ci si deve attenere comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili del trattamento (ai sensi dell'art. 28 del GDPR).

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.

[9] Le funzioni tipiche dell'Amministrazione di un sistema che tratti dati personali erano già richiamate nell'abrogato Allegato B del Codice Privacy.

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 Incaricato della gestione e della manutenzione degli strumenti elettronici (IGSE)

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 Incaricati della gestione e della manutenzione degli strumenti elettronici.

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

L'Incaricato della gestione e della manutenzione degli strumenti elettronici è un Amministratore di sistema che sovrintendere al buon funzionamento delle risorse del sistema informativo e si occupa specificatamente dei sistemi di elaborazione e degli apparati di rete e dei relativi sistemi operativi.

È compito degli Incaricati 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 dell'Incaricato della gestione e della manutenzione degli strumenti elettronici

La nomina dell'Incaricato 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 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 l'Incaricato 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 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 l'Incaricato 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 all'Incaricato 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 (designata anche mediante contratto con altra 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 potrebbero accidentalmente trattare 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 (designata anche mediante contratto con altra persona giuridica, 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; è richiesto il coinvolgimento dell'addetto e la sua sensibilizzazione 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 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 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:

1. 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.
2. 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.
3. Tenere un registro delle persone autorizzate ad accedere ai locali.
4. 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:

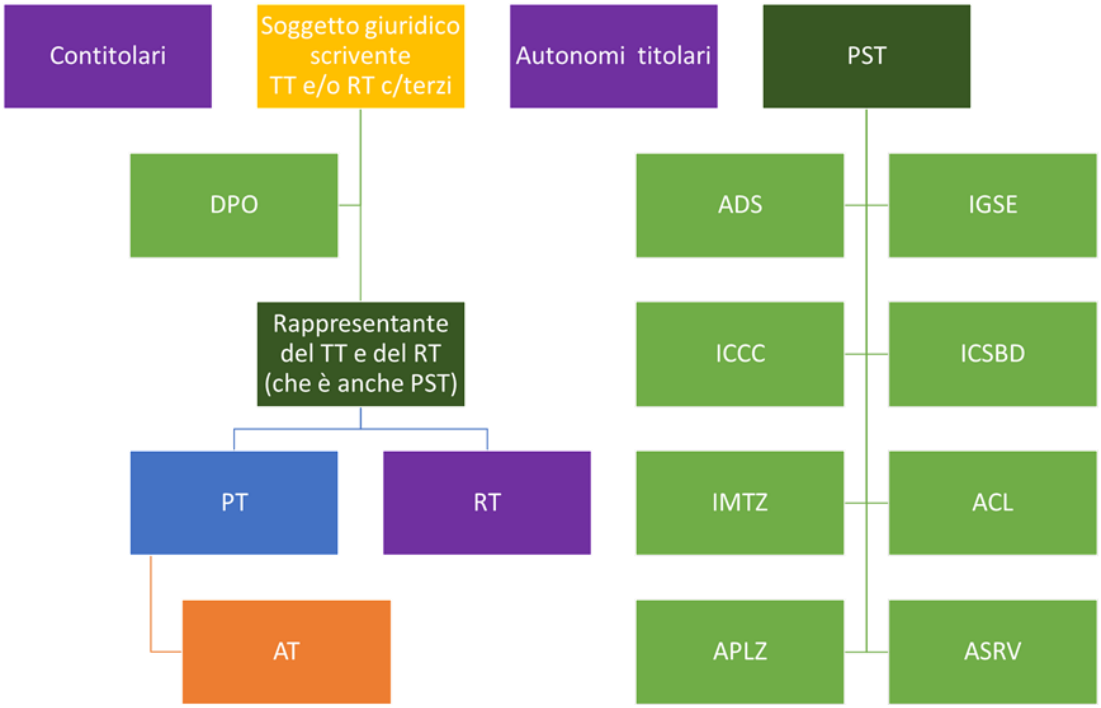
5. Comunicare i propri dati per l'identificazione e registrazione al fine dell'autorizzazione all'accesso.
6. In caso di propria assenza o impedimento, comunicare tempestivamente e ad ogni occasione il nominativo dell'eventuale sostituto.
7. Svolgere le proprie attività limitandosi ai soli compiti assegnati, 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:

- Soggetto giuridico scrivente=INSIT INDUSTRIA SPA (che effettua il trattamento come Titolare o Responsabile del trattamento)
- DPO=Data Protection Officer (assume anche le funzioni del Preposto al riscontro all'interessato (PRI) e Preposto al riscontro al Garante e alla Pubblica Amministrazione (PRG))
- PST=Preposto alla sicurezza del trattamento (interno all'organizzazione)
  - ADS=Amministratore di sistema
  - IGSE=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 dal Rappresentante delegato del TT/RT o PST)
- AT=Autorizzato al trattamento (può essere designato dal Rappresentante delegato del TT/RT o PST o PT)
- RT=Responsabile del trattamento (esterno all'organizzazione; può essere designato dal Rappresentante delegato del TT/RT 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
- Sistema di gestione della sicurezza sul lavoro
- Sistema di gestione della protezione del trattamento di dati
- Sistema di gestione della qualità
- Sistema di gestione di prevenzione dei reati presupposto di cui al D.Lgs. 231/2001
- Sistema informatico e di telecomunicazioni
- Videosorveglianza
- Sito web

- Cause e contenziosi
- INSIT SPA
- Produzione articoli tecnici in gomma e gomma termoplastica
- Smaltimento rifiuti
- Anagrafiche clienti - fornitori
- Portali committenti
- REAT WHISTLEBLOWING
- Logistica
- REAT Immagini e Video

All'interno del dossier "R.E.A.T." oltre le misure di sicurezza generali è riportato l'elenco delle sedi e dei locali.

9.2 Procedure ed istruzioni operative

Il Sistema di gestione e sicurezza delle informazioni

- *Procedura per il monitoraggio e la gestione delle violazioni di dati (Data Breach)*
- *Procedura per la gestione delle richieste degli interessati*
- *Procedura per la distruzione e smaltimento di documenti cartacei contenenti dati personali*
- *Regolamento interno informatico*

9.3 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.

9.4 Accordi, incarichi e designazioni

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

9.5 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
- Altre evidenze di altri sistemi di gestione (es. ISO9001, ISO27001, ecc.)
- Registro degli asset di trattamento dati
- Ecc.

10 Mansionario riferito ai trattamenti di dati personali svolti internamente

Ad integrazione di quanto specificato al paragrafo 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:

- CAPISQUADRA
- DIRIGENTI
- FIDUCIARIO PER WHISTLEBLOWING
- GENERAL MANAGER
- IMPIEGATI ACQUISTI
- IMPIEGATI AMMINISTRATIVI
- IMPIEGATI COMMERCIALI
- IMPIEGATI HR
- IMPIEGATI LOGISTICA
- IMPIEGATI TECNICI
- OPERAI
- OPERAI INTERINALI
- PERSONALE AUTORIZZATO ALL'UTILIZZO, TRASMISSIONE E DIFFUSIONE DI IMMAGINI E VIDEO
- RESPONSABILE IT
- RSPP
- RSU
- TITOLARE

10.1 Categoria: CAPISQUADRA

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 INSIT INDUSTRIA SPA, 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: 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

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- familiari dei lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Produzione articoli tecnici in gomma e gomma termoplastica

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie per: progettare internamente, dati tecnici e programmi utilizzati dai progettisti; analizzare i disegni tecnici forniti dal cliente; industrializzare la produzione; realizzare il prototipo e avviarne la produzione; collaudare i prodotti e fornire report aziendali; gestire e organizzare il magazzino; logistica e spedizione relativa ai prodotti trattati.

Sono altresì presenti le istruzioni da dare agli operai coinvolti nella produzione, collaudo e realizzazione dei prodotti..

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
- Gestione, pianificazione e organizzazione del lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- tecnici
- immagini
- sensibili
- particolari
- soggetti ad accordi di riservatezza

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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: DIRIGENTI

10.2.1 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 INSIT INDUSTRIA SPA, 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: 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

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.3 Categoria: FIDUCIARIO PER WHISTLEBLOWING

10.3.1 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 INSIT INDUSTRIA SPA, 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: REAT WHISTLEBLOWING

Descrizione (ovvero a riguardo di):

.

Gli scopi del trattamento sono:

- Prevenzione di reati ed individuazione di indizi di reato
- Prevenzione su illeciti aziendali

I dati personali trattati sono:

- potenzialmente anche appartenenti a categorie particolari di dati
- relativi a comportamenti illeciti o fraudolenti

Le categorie di persone interessate sono:

- soggetto stesso
- terzi
- lavoratori

Gli asset coinvolti nel trattamento sono:

- piattaforma

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.

10.4 Categoria: GENERAL MANAGER

10.4.1 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 INSIT INDUSTRIA SPA, 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: 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

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: Sistema di gestione della qualità

Descrizione (ovvero a riguardo di):

Documenti, audit, procedure necessari ai corretti adempimenti delle misure previsti dalle norme tecniche riferite alle certificazioni ottenute dall'azienda, in particolare:

- ISO 9001
- ATF 16949
- ISO 14001
- ISO 45001.

Gli scopi del trattamento sono:

- Esigenze di natura organizzativa e produttiva (sistema di qualità automotive ATF 16949 e ISO 9001)
- Salute e sicurezza sul lavoro (ottimizzazione delle procedure ISO 45001)
- Attività commerciale (per dar seguito a richieste specifiche di clienti)
- Tutela dell'ambiente (ISO 14001)

I dati personali trattati sono:

- personali
- personali economici
- dati tecnici

Le categorie di persone interessate sono:

- soggetto stesso

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

- Dispositivo server (virtuale o fisico)

Trattamento n.5: Cause e contenziosi

Descrizione (ovvero a riguardo di):

All'interno della banca dati vengono riportate tutte le informazioni inerenti cause e contenziosi con clienti, lavoratori, collaboratori, fornitori e terzi identificati e/o identificabili..

Gli scopi del trattamento sono:

- Esercitare il diritto di difesa attraverso consulenza legale

I dati personali trattati sono:

- personali
- sensibili
- particolari

Le categorie di persone interessate sono:

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

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo Firewall
- Dispositivo Notebook

Trattamento n.6: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso

- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.7: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.5 Categoria: IMPIEGATI ACQUISTI

10.5.1 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 INSIT INDUSTRIA SPA, 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: Gestione acquisti e approvvigionamenti

Descrizione (ovvero a riguardo di):

Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori.

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)
- Esigenze di natura organizzativa e produttiva
- Salute e sicurezza sul lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- fornitori
- potenziali fornitori
- lavoratori (dei fornitori)

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS

- Dispositivo Firewall

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.

10.6 Categoria: IMPIEGATI AMMINISTRATIVI

10.6.1 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 INSIT INDUSTRIA SPA, 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: 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

Le 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.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.7 Categoria: IMPIEGATI COMMERCIALI

10.7.1 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 INSIT INDUSTRIA SPA, 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: Gestione commerciale e marketing

Descrizione (ovvero a riguardo di):

Offerte, fatture, parcelle, comunicazioni a clienti e potenziali clienti, marketing.

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
- Esigenze di natura organizzativa e produttiva
- Attività commerciale

I dati personali trattati sono:

- personali
- personali economici

Le categorie di persone interessate sono:

- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.8 Categoria: IMPIEGATI HR

10.8.1 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 INSIT INDUSTRIA SPA, 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: 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

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- familiari dei lavoratori

Il trattamento è riferito alle seguenti specificazioni/limitazioni: gestione dati del personale

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.2: 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.3: 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.4: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.9 Categoria: IMPIEGATI LOGISTICA

10.9.1 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 INSIT INDUSTRIA SPA, 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: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.4: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.5: Logistica

Descrizione (ovvero a riguardo di):

Sono presenti tutte le informazioni necessarie per la gestione del ricevimento e spedizione dei prodotti..

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
- Gestione logistica

I dati personali trattati sono:

- personali
- personali economici
- potenzialmente anche appartenenti a categorie particolari di dati (eventuali qualora si verificassero problematiche a livello legale da gestire durante i processi di gestione)

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Servizio Server in cloud

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.

10.10 Categoria: IMPIEGATI TECNICI

10.10.1 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 INSIT INDUSTRIA SPA, 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: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.4: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.11 Categoria: OPERAI

10.11.1 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 INSIT INDUSTRIA SPA, 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: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.4: Produzione articoli tecnici in gomma e gomma termoplastica

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie per: progettare internamente, dati tecnici e programmi utilizzati dai progettisti; analizzare i disegni tecnici forniti dal cliente; industrializzare la produzione; realizzare il prototipo e avviarne la produzione; collaudare i prodotti e fornire report aziendali; gestire e organizzare il magazzino; logistica e spedizione relativa ai prodotti trattati.

Sono altresì presenti le istruzioni da dare agli operai coinvolti nella produzione, collaudo e realizzazione dei prodotti..

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
- Gestione, pianificazione e organizzazione del lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- tecnici
- immagini
- sensibili
- particolari
- soggetti ad accordi di riservatezza

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.12 Categoria: OPERAI INTERINALI

10.12.1 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 INSIT INDUSTRIA SPA, 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: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.4: Produzione articoli tecnici in gomma e gomma termoplastica

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie per: progettare internamente, dati tecnici e programmi utilizzati dai progettisti; analizzare i disegni tecnici forniti dal cliente; industrializzare la produzione; realizzare il prototipo e avviarne la produzione; collaudare i prodotti e fornire report aziendali; gestire e organizzare il magazzino; logistica e spedizione relativa ai prodotti trattati.

Sono altresì presenti le istruzioni da dare agli operai coinvolti nella produzione, collaudo e realizzazione dei prodotti..

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
- Gestione, pianificazione e organizzazione del lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- tecnici
- immagini
- sensibili
- particolari
- soggetti ad accordi di riservatezza

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

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.

10.13 Categoria: PERSONALE AUTORIZZATO ALL'UTILIZZO, TRASMISSIONE E DIFFUSIONE DI IMMAGINI E VIDEO

10.13.1 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 INSIT INDUSTRIA SPA, 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: REAT Immagini e Video

Descrizione (ovvero a riguardo di):

All'interno del REAT sono trattati le immagini e i video acquisiti attraverso i sistemi di videosorveglianza, raccolti per finalità legate alla formazione del personale (attraverso specifiche sessioni di formazione in cui vengono ripresi i lavoratori), per finalità legate alla verifica del ciclo di produzione per lavoratori soggetti a specifici protocolli di sorveglianza sanitaria (immagini e video possono essere trasferiti al medico competente) e per finalità legate a comunicazione e promozione dell'azienda..

Gli scopi del trattamento sono:

- finalità legate alla formazione del personale
- finalità legate alla verifica del ciclo di produzione per lavoratori soggetti a specifici protocolli di sorveglianza sanitaria
- per finalità legate a comunicazione e promozione dell'azienda

I dati personali trattati sono:

- immagini personali
- riprese video

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- terzi identificati e identificabili

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.

10.14 Categoria: RESPONSABILE IT

10.14.1 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 INSIT INDUSTRIA SPA, 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 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)

Le categorie di persone interessate sono:

- soggetto stesso
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Servizio Firewall
- Servizio Software (antivirus)

Trattamento n.2: Videosorveglianza

Descrizione (ovvero a riguardo di):

Riprese di aree in cui potrebbero comparire lavoratori o terzi, identificati o identificabili.

Si specifica che, al sistema di videosorveglianza, possono accedere, in tempo reale, gli addetti che operano nell'ufficio del personale, nell'aera recaption, nell'aministrazione, nel locale spedizioni e, qualora ne avesse necessità, l'ufficio tecnico attraverso specifica richiesta..

Gli scopi del trattamento sono:

- Prevenzione di reati ed individuazione di indizi di reato
- Sicurezza e tutela del patrimonio (dell'ente, di terzi e delle persone)
- Sicurezza e tutela dell'incolumità delle persone
- Sorveglianza (sistematica) di una zona accessibile al pubblico

I dati personali trattati sono:

- personali
- immagini personali
- idonei a rilevare la posizione di beni, strumenti, oggetti
- idonei a rilevare la posizione di persone
- relativi a comportamenti illeciti o fraudolenti

Le categorie di persone interessate sono:

- utenti
- lavoratori
- clienti
- fornitori
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Dispositivo Digital Video Recorder e impianto TVCC-over-IP

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.

10.15 Categoria: RSPP

10.15.1 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 INSIT INDUSTRIA SPA, 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

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.

10.16 Categoria: RSU

10.16.1 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 INSIT INDUSTRIA SPA, 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: Videosorveglianza

Descrizione (ovvero a riguardo di):

Riprese di aree in cui potrebbero comparire lavoratori o terzi, identificati o identificabili.

Si specifica che, al sistema di videosorveglianza, possono accedere, in tempo reale, gli addetti che operano nell'ufficio del personale, nell'aera recaption, nell'aministrazione, nel locale spedizioni e, qualora ne avesse necessità, l'ufficio tecnico attraverso specifica richiesta..

Gli scopi del trattamento sono:

- Prevenzione di reati ed individuazione di indizi di reato
- Sicurezza e tutela del patrimonio (dell'ente, di terzi e delle persone)
- Sicurezza e tutela dell'incolumità delle persone
- Sorveglianza (sistematica) di una zona accessibile al pubblico

I dati personali trattati sono:

- personali
- immagini personali
- idonei a rilevare la posizione di beni, strumenti, oggetti
- idonei a rilevare la posizione di persone
- relativi a comportamenti illeciti o fraudolenti

Le categorie di persone interessate sono:

- utenti
- lavoratori
- clienti
- fornitori
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Dispositivo Digital Video Recorder e impianto TVCC-over-IP

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.

10.17 Categoria: TITOLARE

10.17.1 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: 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

Le 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

Le 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)

Le 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

Le 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

Le 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: Gestione commerciale e marketing

Descrizione (ovvero a riguardo di):

Offerte, fatture, parcelle, comunicazioni a clienti e potenziali clienti, marketing.

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
- Esigenze di natura organizzativa e produttiva
- Attività commerciale

I dati personali trattati sono:

- personali
- personali economici

Le categorie di persone interessate sono:

- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.7: Gestione acquisti e approvvigionamenti

Descrizione (ovvero a riguardo di):

Offerte, fatture, documenti di trasporto, comunicazioni a fornitori e potenziali fornitori.

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)
- Esigenze di natura organizzativa e produttiva
- Salute e sicurezza sul lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- fornitori
- potenziali fornitori
- lavoratori (dei fornitori)

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.8: 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.9: 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.10: Sistema di gestione della qualità

Descrizione (ovvero a riguardo di):

Documenti, audit, procedure necessari ai corretti adempimenti delle misure previsti dalle norme tecniche riferite alle certificazioni ottenute dall'azienda, in particolare:
- ISO 9001
- ATF 16949
- ISO 14001
- ISO 45001.

Gli scopi del trattamento sono:
- Esigenze di natura organizzativa e produttiva (sistema di qualità automotive ATF 16949 e ISO 9001)
- Salute e sicurezza sul lavoro (ottimizzazione delle procedure ISO 45001)
- Attività commerciale (per dar seguito a richieste specifiche di clienti)
- Tutela dell'ambiente (ISO 14001)

I dati personali trattati sono:
- personali
- personali economici
- dati tecnici

Le categorie di persone interessate sono:
- soggetto stesso

Gli asset coinvolti nel trattamento sono:
- Dispositivo Personal Computer
- Dispositivo server (virtuale o fisico)

Trattamento n.11: 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

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer

Trattamento n.12: 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)

Le categorie di persone interessate sono:

- soggetto stesso
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Servizio Firewall
- Servizio Software (antivirus)

Trattamento n.13: Videosorveglianza

Descrizione (ovvero a riguardo di):

Riprese di aree in cui potrebbero comparire lavoratori o terzi, identificati o identificabili.

Si specifica che, al sistema di videosorveglianza, possono accedere, in tempo reale, gli addetti che operano nell'ufficio del personale, nell'aera recaption, nell'aministrazione, nel locale spedizioni e, qualora ne avesse necessità, l'ufficio tecnico attraverso specifica richiesta..

Gli scopi del trattamento sono:

- Prevenzione di reati ed individuazione di indizi di reato
- Sicurezza e tutela del patrimonio (dell'ente, di terzi e delle persone)
- Sicurezza e tutela dell'incolumità delle persone
- Sorveglianza (sistematica) di una zona accessibile al pubblico

I dati personali trattati sono:

- personali
- immagini personali
- idonei a rilevare la posizione di beni, strumenti, oggetti
- idonei a rilevare la posizione di persone
- relativi a comportamenti illeciti o fraudolenti

Le categorie di persone interessate sono:

- utenti
- lavoratori
- clienti
- fornitori
- terzi identificati e identificabili

Il trattamento è riferito alle seguenti specificazioni/limitazioni: dententrice di metà password per l'accesso ai sistemi informativi

Gli asset coinvolti nel trattamento sono:

- Dispositivo Digital Video Recorder e impianto TVCC-over-IP

Trattamento n.14: Sito web

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.

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)

Le categorie di persone interessate sono:

- utenti
- terzi identificati e identificabili

Gli asset coinvolti nel trattamento sono:

- Servizio Applicazione web (sito web)

Trattamento n.15: Cause e contenziosi

Descrizione (ovvero a riguardo di):

All'interno della banca dati vengono riportate tutte le informazioni inerenti cause e contenziosi con clienti, lavoratori, collaboratori, fornitori e terzi identificati e/o identificabili..

Gli scopi del trattamento sono:

- Esercitare il diritto di difesa attraverso consulenza legale

I dati personali trattati sono:

- personali
- sensibili
- particolari

Le categorie di persone interessate sono:

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

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo Firewall
- Dispositivo Notebook

Trattamento n.16: INSIT SPA

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie alla gestione dei locali, dell'attività e delle attrezzature, compresi contratti di manutenzione (ordinaria e straordinaria), ciclo di produzione dei lavoratori, orari e tutte le informazioni necessarie per lo svolgimento dell'attività e per l'interfacciamento con clienti e fornitori..

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)
- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali
- sensibili
- particolari
- tecnici
- personali economici

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- clienti

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.17: Produzione articoli tecnici in gomma e gomma termoplastica

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie per: progettare internamente, dati tecnici e programmi utilizzati dai progettisti; analizzare i disegni tecnici forniti dal cliente; industrializzare la produzione; realizzare il prototipo e avviarne la produzione; collaudare i prodotti e fornire report aziendali; gestire e organizzare il magazzino; logistica e spedizione relativa ai prodotti trattati.

Sono altresì presenti le istruzioni da dare agli operai coinvolti nella produzione, collaudo e realizzazione dei prodotti..

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
- Gestione, pianificazione e organizzazione del lavoro
- Gestione logistica

I dati personali trattati sono:

- personali
- tecnici
- immagini
- sensibili
- particolari
- soggetti ad accordi di riservatezza

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- potenziali clienti
- fornitori
- potenziali fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.18: Smaltimento rifiuti

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le informazioni necessarie per lo smaltimento dei rifiuti..

Gli scopi del trattamento sono:

- Smaltimento dei rifiuti

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo Firewall
- Dispositivo NAS

Trattamento n.19: Anagrafiche clienti - fornitori

Descrizione (ovvero a riguardo di):

All'interno della banca dati sono contenute tutte le anagrafiche di clienti e fornitori.

Sono altresì contenute tutte le informazioni in merito ai contratti, articoli e prodotti proposti, prezzi, tipologie di distribuzione e logistica, servizi gestiti da terzi e tutte le informazioni necessarie per regolare i rapporti tra le parti..

Gli scopi del trattamento sono:

- Gestione, pianificazione e organizzazione del lavoro

I dati personali trattati sono:

- personali

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Dispositivo NAS
- Dispositivo Firewall

Trattamento n.20: REAT WHISTLEBLOWING

Descrizione (ovvero a riguardo di):

.

Gli scopi del trattamento sono:

- Prevenzione di reati ed individuazione di indizi di reato
- Prevenzione su illeciti aziendali

I dati personali trattati sono:

- potenzialmente anche appartenenti a categorie particolari di dati
- relativi a comportamenti illeciti o fraudolenti

Le categorie di persone interessate sono:

- soggetto stesso
- terzi
- lavoratori

Gli asset coinvolti nel trattamento sono:

- piattaforma

Trattamento n.21: Logistica

Descrizione (ovvero a riguardo di):

Sono presenti tutte le informazioni necessarie per la gestione del ricevimento e spedizione dei prodotti..

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
- Gestione logistica

I dati personali trattati sono:

- personali
- personali economici
- potenzialmente anche appartenenti a categorie particolari di dati (eventuali qualora si verificassero problematiche a livello legale da gestire durante i processi di gestione)

Le categorie di persone interessate sono:

- soggetto stesso
- clienti
- fornitori

Gli asset coinvolti nel trattamento sono:

- Dispositivo Personal Computer
- Dispositivo Server fisico
- Servizio Server in cloud

Trattamento n.22: REAT Immagini e Video

Descrizione (ovvero a riguardo di):

All'interno del REAT sono trattati le immagini e i video acquisiti attraverso i sistemi di videosorveglianza, raccolti per finalità legate alla formazione del personale (attraverso specifiche sessioni di formazione in cui vengono ripresi i lavoratori), per finalità legate alla verifica del ciclo di produzione per lavoratori soggetti a specifici protocolli di sorveglianza sanitaria (immagini e video possono essere trasferiti al medico competente) e per finalità legate a comunicazione e promozione dell'azienda..

Gli scopi del trattamento sono:

- finalità legate alla formazione del personale
- finalità legate alla verifica del ciclo di produzione per lavoratori soggetti a specifici protocolli di sorveglianza sanitaria
- per finalità legate a comunicazione e promozione dell'azienda

I dati personali trattati sono:

- immagini personali
- riprese video

Le categorie di persone interessate sono:

- soggetto stesso
- lavoratori
- terzi identificati e identificabili

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.

10.17.2 Ambito Responsabile del trattamento

10.18 Ulteriori istruzioni per gli Autorizzati

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 al paragrafo 10, debbono in particolare osservare le seguenti disposizioni:

- divieto di trattare i dati a chiunque agisce sotto l'autorità dell'organizzazione di INSIT INDUSTRIA SPA e abbia accesso a tali dati personali se non è stato istruito;
- 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;
- divieto di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale extra-UE in assenza o di una decisione di adeguatezza ai sensi dell'art.45 o di garanzie adeguate ai sensi dell'art.46 o di norme vincolanti d'impresa ai sensi dell'art.47 o di applicazione delle deroghe dell'art.49 con riferimento al Reg.(UE) n. 2016/679;
- la comunicazione dei dati a terzi avviene solo se prevista da obblighi di legge, dagli accordi contrattuali o comunque consentita dagli interessati;
- 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 nomina ad Autorizzato al trattamento, ma anche per tutto il tempo successivo durante il quale sarà in vigore tale divieto, senza limiti temporali;
- ogni persona autorizzata al trattamento ha l'obbligo di osservanza e contribuzione all'attuazione del Sistema di gestione;
- ogni persona autorizzata al trattamento deve informare tempestivamente il Titolare o il Preposto o il Responsabile in caso di violazioni dei dati personali o incidenti di sicurezza.

Si raccomanda inoltre a ogni persona autorizzata al trattamento di dati personali di segnalare tempestivamente e in maniera circostanziata ogni situazione che a proprio avviso:

- non sia conforme alla normativa rilevante in materia di protezione dei dati personali o di riservatezza e segretezza delle informazioni ovvero alle politiche adottate al riguardo (codesto modello organizzativo, politica, procedure, ecc.);
- non garantisca misure di sicurezza adeguate al rischio per i diritti e le libertà fondamentali delle persone interessate al trattamento;
- riconosca comportamenti non conformi alle presenti disposizioni.

11 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:

- AGENZIE INTERINALI
- ASSISTENZA PER LO SMALTIMENTO RIFIUTI
- Assicurazioni
- Assistenza programma informatico
- Assistenza sistema informatico
- Banche
- COLLEGIO DEI REVISORI / SINDACI
- Commercialista ed elaborazione contabilità
- Compagnie telefoniche
- Connettività internet
- Consulente Privacy
- Consulente Sicurezza sul lavoro
- Consulente lavoro ed elaborazione paghe
- Consulente per la qualità
- ELABORAZIONE MODELLI INTRASTAT
- FORNITORE INSTALLAZIONE VIDEOSORVEGLIANZA
- FORNITORE PIATTAFORMA PER WHISTLEBLOWING
- FORNITORE SERVER
- GESTORE DELLA STRUMENTAZIONE ELETTRONICA
- Medico competente
- ORGANISMO DI VIGILANZA
- PORTALE COMMITTENTE
- Provider PEC
- Provider dominio internet
- Provider posta elettronica
- Studio legale
- Trasporti e spedizioni

- Webmaster

11.1 Categoria: AGENZIE INTERINALI

Tale categoria è assegnata ai seguenti trattamenti:

- Selezione del personale come Responsabile del trattamento

11.2 Categoria: ASSISTENZA PER LO SMALTIMENTO RIFIUTI

Tale categoria è assegnata ai seguenti trattamenti:

- Smaltimento rifiuti come Responsabile del trattamento

11.3 Categoria: Assicurazioni

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Destinatario Autonomo Titolare del trattamento

11.4 Categoria: Assistenza programma informatico

Tale categoria è assegnata ai seguenti trattamenti:

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

11.5 Categoria: Assistenza sistema informatico

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Autorizzato al trattamento; riferito alle seguenti specificazioni/limitazioni: limitatamente alla manutenzione e configurazione del sistema e della rete

11.6 Categoria: Banche

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Destinatario Autonomo Titolare del trattamento

- Anagrafiche clienti - fornitori come Destinatario Autonomo Titolare del trattamento

11.7 Categoria: COLLEGIO DEI REVISORI / SINDACI

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Autorizzato al trattamento

11.8 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

11.9 Categoria: Compagnie telefoniche

Tale categoria è assegnata ai seguenti trattamenti:

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

11.10 Categoria: Connettività internet

Tale categoria è assegnata ai seguenti trattamenti:

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

11.11 Categoria: Consulente Privacy

Tale categoria è assegnata ai seguenti trattamenti:

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

11.12 Categoria: Consulente Sicurezza sul lavoro

Tale categoria è assegnata ai seguenti trattamenti:

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

11.13 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

11.14 Categoria: Consulente per la qualità

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della qualità come Responsabile del trattamento

11.15 Categoria: ELABORAZIONE MODELLI INTRASTAT

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione amministrativo-contabile come Responsabile del trattamento
- Logistica come Responsabile del trattamento

11.16 Categoria: FORNITORE INSTALLAZIONE VIDEOSORVEGLIANZA

Tale categoria è assegnata ai seguenti trattamenti:

- Videosorveglianza come Responsabile del trattamento
- REAT Immagini e Video come Autorizzato al trattamento

11.17 Categoria: FORNITORE PIATTAFORMA PER WHISTLEBLOWING

Tale categoria è assegnata ai seguenti trattamenti:

- REAT WHISTLEBLOWING come Responsabile del trattamento

11.18 Categoria: FORNITORE SERVER

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Responsabile del trattamento

11.19 Categoria: GESTORE DELLA STRUMENTAZIONE ELETTRONICA

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema informatico e di telecomunicazioni come Responsabile del trattamento

11.20 Categoria: Medico competente

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della sicurezza sul lavoro come Responsabile del trattamento
- REAT Immagini e Video come Destinatario Autonomo Titolare del trattamento

11.21 Categoria: ORGANISMO DI VIGILANZA

Tale categoria è assegnata ai seguenti trattamenti:

- Sistema di gestione della qualità come Autorizzato al trattamento
- Smaltimento rifiuti come Autorizzato al trattamento

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

11.22 Categoria: PORTALE COMMITTENTE

Tale categoria è assegnata ai seguenti trattamenti:

- Portali committenti come Titolare del trattamento

11.23 Categoria: Provider PEC

Tale categoria è assegnata ai seguenti trattamenti:

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

11.24 Categoria: Provider dominio internet

Tale categoria è assegnata ai seguenti trattamenti:

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

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

11.25 Categoria: Provider posta elettronica

Tale categoria è assegnata ai seguenti trattamenti:

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

11.26 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

- Cause e contenziosi come Responsabile del trattamento

11.27 Categoria: Trasporti e spedizioni

Tale categoria è assegnata ai seguenti trattamenti:

- Gestione attività di segreteria generale come Destinatario Autonomo Titolare del trattamento

11.28 Categoria: Webmaster

Tale categoria è assegnata ai seguenti trattamenti:

- Sito web come Responsabile del trattamento