N. - Ed. - Rev.	**508357 1 3**	Destinatari:	**Tutte le funzioni ed unità aziendali delle Società del gruppo Sirti**
Sez:	-		
Classificazione	**SG PO PE**		
Data emissione	**11/01/2024**	e p.c.	**AD**
Liv.Riservatezza:	**INTERNAL**		

PRIVACY

Disposizioni generali per l'applicazione della normativa Privacy in Azienda

La presente policy definisce le disposizioni e le modalità operative in materia di trattamento di dati personali in ottemperanza al Regolamento EU n. 2016/679, al D.Lgs. 101/2018 ed ai Provvedimenti del

Garante Privacy, nonché fornisce le linee guida sulle quali dovranno basarsi eventuali ulteriori procedure e normative aziendali.

Privacy
Disposizioni generali per l'applicazione della normativa Privacy

GESTIONE	FUNZIONE	FIRMATARI
REDATTO	*Funzione Compliance*	Giorgia Briamonte
APPROVATO	*Group Corporate, Legal, Public & Tax Affairs*	Michele Scibetta
EMESSO	*Organizational Design & Continuous Improvement*	Patrizia Zepponi
N. allegati	-	

Il presente documento è stato redatto in coerenza con il Codice Etico del Gruppo Sirti e il Modello Organizzativo 231 delle Società del Gruppo Sirti

Registro delle Revisioni
Le eventuali edizioni o revisioni di documenti cartacei superati vanno distrutte o, se necessario, conservate separatamente; sui documenti superati va posta la dizione “ANNULLATO”

ED.	REV.	DATA	DESCRIZIONE
1	0	03/08/2016	Emissione. La presente sostituisce la procedura 258766 sez. 1 – 20
1	1	30/08/2018	Revisione. Adeguamento Policy al nuovo Regolamento EU n. 2016/679
1	2	15/11/2021	Revisione. Adeguamento Policy a seguito di aggiornamenti normativi
1	3	11/01/2024	Revisione. Adeguamento aggiornamenti interni struttura Privacy-Estensione Policy a Wellcomm Engineering

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

La presente Policy ha lo scopo di definire le disposizioni e le modalità operative in materia di trattamento di dati personali, in ottemperanza al Regolamento (EU) n. 2016/679 ("GDPR") ed al D.Lgs 101/2018 che adegua il Codice Privacy (Decreto Legislativo 30 giugno 2003, n. 196) alle disposizioni del suddetto Regolamento, nonché di fornire le linee guida sulle quali dovranno basarsi eventuali ulteriori procedure e normative aziendali.

La normativa sulla privacy recepisce il c.d. "*General Data Protection Regulation - GDPR*" pubblicato con il Regolamento Europeo n. 2016/679 ed il Decreto Legislativo 10 agosto 2018 n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

2. DESTINATARI

La Policy è rivolta alle Società del Gruppo Sirti (di seguito genericamente "la Società") ed ai suoi dipendenti. Le sue disposizioni si applicano ai "trattamenti" effettuati nell'ambito del territorio dello Stato italiano e si applicano, altresì, in caso di trasferimento di dati personali da e verso l'estero (Paesi Ue ed extra Ue).

3. RIFERIMENTI

- Policy Information Security n. 508358. Fornisce le linee guida per la sicurezza delle informazioni aziendali
- Procedura Gestione della Sicurezza sul lavoro – visite mediche – n. 500836 sez. 3
- Modello di Organizzazione, Gestione e Controllo ai sensi dell'art. 6, comma 3°, del Decreto Legislativo 8 giugno 2001 n.231 e successive integrazioni delle Società del Gruppo Sirti
- Codice Etico Gruppo Sirti

Solo per la società Wellcomm Engineering:

- Regolamento Informatico Aziendale

Organigramma privacy

4. QUADRO NORMATIVO DI RIFERIMENTO

- Regolamento Europeo n. 2016/679 "General Data Protection Regulation" (c.d. "GDPR").
- Decreto Legislativo 10 agosto 2018 n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*"
- Provvedimento del Garante del 27 novembre 2008 in materia di Amministratori di Sistema
- Provvedimento del Garante in materia del lavoro e previdenza sociale (Informativa degli annunci relativi a offerte di lavoro) del 10 gennaio 2002
- Provvedimento del Garante del 08 aprile 2010 in materia di videosorveglianza
- Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate il 29 gennaio 2020.

5. PRINCIPALI DEFINIZIONI

Di seguito le principali definizioni previste dal GDPR e dal D.Lgs. 101/2018:

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.

Anche la semplice conservazione di un dato ed anche la sua consultazione o lettura sono considerati dalla legge "trattamento" e anche la cancellazione o la distruzione fisica del supporto contenente il dato sono "trattamento" del dato stesso.
Tutte le operazioni, siano esse attive (come ad esempio la raccolta di dati attraverso un modulo o la loro comunicazione a terzi), siano esse passive (come il ricevimento tramite e-mail di un curriculum vitae di un candidato all'assunzione; la custodia di documenti cartacei contenenti dati personali in un archivio o in uno schedario) devono rispettare la normativa di tutela privacy.

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.

*Sono considerati "dati personali" sia i **dati identificativi** veri e propri (cioè nome, cognome, indirizzo, denominazione, sede, fotografia, registrazione della voce, impronte digitali, ecc.) sia i **dati finalizzati all'identificazione**, cioè le informazioni che sono oggettivamente idonee ad individuare un determinato soggetto (es. codice fiscale, gli estremi del documento di identità, le coordinate bancarie, l'indirizzo e-mail, ecc.)*

Categorie particolari di dati personali (c.d. "sensibili"): sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale

Sono dati particolari i dati rivolti a:
- rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni di carattere religioso, filosofico, i dati concernenti la fruizione dei permessi e festività religiose o dei servizi mensa;
- rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere politico o sindacale,
- rivelare lo stato di salute del dipendente e dei suoi familiari, i dati raccolti in riferimento a malattie anche professionali, a invalidità, infermità, gravidanza, puerperio, allattamento, dati relativi ad infortuni, ad esposizione a fattori di rischio, all'idoneità psicofisica a svolgere determinate mansioni, dati relativi all'appartenenza a categorie protette.

Dati personali relativi a condanne penali e reati (c.d. "giudiziari"): sono i dati personali che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Si citano a titolo esemplificativo ma non esaustivo: i provvedimenti giudiziari penali di condanna definitivi, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere; i provvedimenti giudiziari concernenti le pene accessorie (interdizione dai pubblici uffici, interdizione/sospensione da una professione o da

un'arte, interdizione legale, incapacità di contrattare con la pubblica amministrazione, decadenza o sospensione della potestà dei genitori, pubblicazione della sentenza penale di condanna);

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

Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO): ha la funzione di affiancare titolare, addetti e responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento Europeo. Viene identificato nella persona fisica avente comprovata esperienza in materia designata dal Titolare a consigliare e sorvegliare il Titolare stesso e funge anche da tramite fra l'organizzazione e l'autorità.
I suoi compiti sono indicati all'articolo 39 del GDPR e sono essenzialmente quelli di informare, sorvegliare e cooperare con il Titolare nella gestione delle problematiche connesse al trattamento dei dati personali.

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; può essere individuato all'interno della società -Responsabile Interno- (qualificato come "Designato" al Trattamento")o/e all'esterno "Responsabile Esterno".

Sub-Responsabile del trattamento: la persona fisica o giuridica che può essere nominata responsabile del trattamento da parte di un Responsabile previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

Autorizzato al trattamento (o persona autorizzata): la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile (*es. i dipendenti della società che trattano dati personali).*

Interessato del trattamento: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (*es. dipendenti, clienti, fornitori, visitatori*).

Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Garante Privacy: è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (Legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento Europeo sulla protezione dei dati personali 2016/679 (art. 51).

Registro Trattamento Dati: ogni Titolare del trattamento e, ove applicabile, il suo Rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità o per conto di un Titolare terzo; il Registro può essere tenuto in forma scritta o elettronica ed è obbligatorio per imprese e organizzazioni con più di 250 dipendenti a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categoria particolari di dati (art.9 – art.10 GDPR).

Violazione di dati personali (Data breach): Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

6. LE FIGURE PRIVACY

Figure che effettuano i trattamenti

Di seguito i soggetti che effettuano trattamenti di dati personali a cui la normativa attribuisce un ruolo ben preciso nel sistema normativo.

Figura privacy	Rif. Normativi	Definizione
TITOLARE	Art. 24 (GDPR)	Il soggetto (persona fisica, società, ente, associazioni, ecc.) che decide autonomamente in ordine alle finalità ed alle modalità di trattamento dei dati personali, ivi compreso le misure di sicurezza e gli strumenti utilizzati.
DATA PROTECTION OFFICER (DPO)	Art. 37-38-39 (GDPR)	Persona fisica designata dal Titolare sulla base delle sue qualità professionali che va ad affiancare il Titolare nella gestione delle problematiche del trattamento dei dati personali.
RESPONSABILE DEL TRATTAMENTO	Art. 28 (GDPR)	Il soggetto (persona fisica o giuridica) preposto dal Titolare al trattamento di dati personali.
SUB-RESPONSABILE DEL TRATTAMENTO	Riferimento in Art. 28 (GDPR)	La persona fisica o giuridica che può essere nominata Responsabile del trattamento da parte di un Responsabile.
DESIGNATO	Art. 29 (GDPR)	La persona fisica che compie materialmente le operazioni di trattamento su incarico del Titolare o del Responsabile.
PERSONA AUTORIZZATA DI I LIVELLO	Art. 29 (GDPR)	La persona fisica che compie materialmente le operazioni di trattamento su incarico del Designato.
PERSONA AUTORIZZATA DI II LIVELLO	Art. 12-13-14-15 (GDPR)	La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali e la quale compie materialmente le operazioni di trattamento.
AMMINISTRATORE DI SISTEMA	Provvedimento del Garante del 27 novembre 2008	La figura professionale, individuata nell'ambito degli Incaricati del Trattamento, dedicata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e a tutte quelle figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati.
FUNZIONE COMPLIANCE	-	È la Funzione aziendale responsabile del presidio interno al Gruppo Sirti della normativa, del coordinamento e monitoraggio in materia di privacy.

6.1 Titolare

Titolare del trattamento è *il soggetto* (persona fisica, società, ente, associazioni, ecc.) *che decide autonomamente in ordine alle finalità ed alle modalità di trattamento dei dati personali, ivi* compreso le misure di sicurezza e gli strumenti utilizzati.

Nel caso di persona giuridica, il Titolare del trattamento è la **singola società** e non le persone fisiche che l'amministrano o che la rappresentano (quali ad esempio l'Amministratore Delegato, il Presidente, il Legale Rappresentante).

Essendo il Titolare il centro di imputazione degli obblighi e delle responsabilità attribuitigli dal GDPR è, al tempo stesso, il principale destinatario delle sanzioni per il mancato rispetto delle norme previste in materia di protezione dei dati personali.

La titolarità non è delegabile, in quanto tale, ciò che può essere oggetto di delega è l'esercizio dei poteri o, meglio, di alcuni poteri del Titolare**;** il Titolare può nominare infatti un **DPO** e dei **Responsabili al Trattamento dei dati.**

All'interno del Gruppo Sirti, ogni singola Società si identifica come Titolare del trattamento dei dati personali dei propri dipendenti, clienti e fornitori. Ogni Società ha un proprio "Organigramma Privacy".

6.2 Data Protection Officer (DPO)

Il DPO è la figura introdotta dal Regolamento Europeo in materia di protezione dei dati personali che ricopre il ruolo di consulente esperto andando ad affiancare il Titolare nella gestione delle problematiche del trattamento dei dati personali; può essere interno all'azienda o un consulente esterno.
Il DPO deve essere coinvolto in tutte le questioni inerenti la protezione dei dati nonché sostenuto nell'esecuzione dei suoi compiti dal Titolare e dal Responsabile del trattamento che gli devono fornire tutte le risorse necessarie per svolgere la sua attività. Il lavoro del DPO deve svolgersi in assoluta autonomia e indipendenza.

All'interno del Gruppo Sirti è stato nominato come DPO di Sirti S.p.A., Sirti Telco Infrastructures S.p.A., Sirti Digital Solutions S.p.A.. Sirti Alliance for Infrastructures, Sirti Telco Piemonte e Wellcomm lo Studio Legale 42 LawFirm S.r.l. - Società tra Avvocati,

6.3 Responsabile del trattamento dei dati

Nelle grandi realtà aziendali difficilmente vi è una gestione diretta da parte del Titolare di tutte le operazioni legate al corretto adempimento della normativa sulla privacy; infatti, la stessa normativa privacy prevede la possibilità di individuare una figura che collabori con il Titolare del trattamento per dare concretamente attuazione alla normativa. Si tratta del **Responsabile del trattamento.** Proprio al fine di assicurare un elevato livello di tutela dei dati personali, la nomina diventa fondamentale per tutte le strutture organizzative complesse e articolate.

Il Responsabile del trattamento, che può essere individuato sia all'interno ("Designato") che all'esterno ("Responsabile Esterno") dell'organizzazione, può essere nominato solo dal Titolare.

I soggetti da nominare (siano essi persone fisiche che giuridiche) devono essere individuati tra quelli 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.

Ai fini dell'applicazione della normativa in materia di privacy, non è previsto un rapporto di tipo gerarchico tra i vari Responsabili del trattamento interni e/o esterni nominati. Ognuno di essi, a prescindere dalla posizione gerarchica ricoperta nella struttura aziendale, risponde direttamente al Titolare per i trattamenti di competenza.

L'inosservanza delle disposizioni di cui alla presente Policy e delle istruzioni riportate nella lettera di nomina possono esporre il Titolare e lo stesso Responsabile (Interno e/o Esterno) al rischio di sanzioni, anche di natura penale, oltre ad arrecare possibili danni all'immagine della Società.

Ogni Società del Gruppo Sirti ha individuato dei propri Designati e Responsabili Esterni.

6.3.1 Designato al trattamento dati personali

Nomina

Per i trattamenti effettuati all'interno della Società sono, di norma, nominati "*Designati*" i primi riporti del vertice aziendale (n-1) e/o soggetti che, in base al ruolo aziendale di cd. "Responsabili di Funzione" e alla comprovata esperienza in materia, sono titolati ad assumere tale nomina.

La Funzione *Compliance,* sulla base delle motivazioni addotte e dei trattamenti per i quali si propone la nomina dei Designati, procede all'eventuale predisposizione della nomina.

Competenze e responsabilità

Le competenze e le responsabilità attribuite ai Designati del trattamento sono rappresentate essenzialmente dai compiti e dagli adempimenti specificati nella lettera di nomina.

In alternativa, nelle istruzioni possono essere indicati i riferimenti delle procedure in cui dette disposizioni sono descritte.

I Designati devono:

- garantire che la gestione dei dati personali avvenga nel rispetto della Normativa di Settore attenendosi scrupolosamente alle istruzioni a lui impartite dal Titolare;
- rispettare i principi di necessità, adeguatezza, pertinenza e non eccedenza nello svolgimento delle attività di trattamento dei dati personali;
- verificare e provvedere in merito alla corretta comunicazione agli Interessati dell'informativa di cui agli artt. 13 e 14 del RGPD nonché all'eventuale raccolta del consenso, ove necessario;
- supervisionare i soggetti appartenenti alla propria unità (cd. Autorizzati di I° livello) che, nell'ambito dell'assetto organizzativo del Titolare e sotto l'autorità dello stesso, siano preposti a specifici trattamenti dei dati e fornire agli stessi istruzioni per la corretta elaborazione dei Dati personali, sovrintendendo e vigilando l'attuazione delle istruzioni impartite;
- curare il coordinamento di tutte le operazioni sui Dati affidate agli Autorizzati di I° livello;
- collaborare con il Responsabile per la Protezione dei Dati personali (di seguito denominato "RPD"), con i soggetti preposti alla verifica e all'esecuzione degli adempimenti in materia di privacy (di seguito denominati "Referenti Privacy") nonché con le Autorità preposte alla verifica e sorveglianza dell'applicazione del RGPD, per l'attuazione, l'introduzione e il mantenimento delle misure tecniche e organizzative in conformità all'art. 32 del RGPD;
- curare l'aggiornamento formativo periodico in materia di disciplina della protezione dei dati e di sicurezza, secondo le modalità che verranno indicate dal RPD;
- istruire, anche su richiesta del Titolare, gli Autorizzati di I° livello sulle modalità di trattamento con riferimento all'adozione e all'osservanza delle specifiche misure di sicurezza;
- procedere a verifiche periodiche in merito al pieno rispetto da parte degli Autorizzati di I° livello delle istruzioni impartite e della Normativa Applicabile;
- riferire prontamente al Titolare in merito a qualunque elemento, questione o richiesta da parte di un Interessato del trattamento (di seguito denominato "Interessato") che possa comportare la responsabilità del Titolare in merito ad uno dei trattamenti svolti;
- coordinarsi con gli altri Designati nominati dal Titolare, con il RPD e con i Referenti Privacy al fine di garantire il corretto espletamento delle procedure e il rispetto della Normativa Applicabile;
- garantire il rispetto delle misure di sicurezza prescritte dal Titolare in merito al trattamento svolto.

La lettera di nomina a Designato contenente le relative istruzioni operative viene predisposta, su incarico e previa valutazione del Titolare, dalla Funzione *Compliance* che provvede anche all'archiviazione della nomina e alle registrazioni nel sistema informativo.

Validità e revoca della nomina

La nomina, salvo revoca espressa, ha **validità** fino ad eventuale trasferimento del Designato ad una nuova attività; in tal caso la Funzione *Compliance*, su indicazione del Titolare, provvederà ad emettere una nuova nomina.

In caso di cessazione del rapporto di lavoro, la revoca avviene automaticamente e tacitamente.

6.3.2 Responsabile Esterno del trattamento dati personali

La nomina a Responsabile Esterno deve avvenire in tutti i casi in cui un terzo effettua trattamenti di dati personali per conto della Società e non può essere considerato come autonomo Titolare o come Autorizzato al trattamento.

Il Responsabile Esterno può essere persona fisica o giuridica.

I trattamenti esternalizzati devono essere disciplinati da un contratto o atto giuridico ("Data Processing Agreement" o "Nomina a Responsabile Esterno al trattamento dati personali") scritto e sottoscritto per accettazione, nel quale vengono riportate le competenze e le responsabilità del Responsabile Esterno, nonché le misure di sicurezza/istruzioni tecniche che lo stesso dovrà adottare nel trattamento dei dati personali per conto del Titolare.

I Responsabili Esterni hanno gli stessi compiti dei Responsabili Interni (vedi par. 6.3.1 "Competenze e Responsabilità").

a) Nomina a "Responsabile Esterno al trattamento dati personali di un terzo" da parte di una Società del Gruppo

Qualora il trattamento di dati personali venga effettuato da un terzo (persona fisica o giuridica), il terzo deve essere incaricato dalla Società, in qualità di Titolare del trattamento dei dati, tramite apposita nomina a "Responsabile Esterno al trattamento dati personali" contenuta all'interno del cd. "Data Processing Agreement" predisposto dalla Funzione *Compliance* su indicazione del Titolare.

La Funzione Procurement & Supply Chain provvede ad inviare al terzo il suddetto atto che deve essere restituito compilato e firmato alla casella di posta elettronica privacy@sirti.it; una volta ricevuto l'atto controfirmato, la Funzione effettua, su indicazione del Titolare e/o del Responsabile Interno, una valutazione nel merito dell'atto e - se ritenuto correttamente compilato da parte del fornitore e compliant alla normativa vigente in materia di privacy, nonché a quanto previsto dalle policy aziendali vigenti in materia privacy – provvede alla finalizzazione del documento e alla relativa registrazione dell'atto, debitamente firmato dalle parti, nell'apposito Registro Trattamento Dati.

Come esempi, può essere nominato Responsabile Esterno il consulente del lavoro che elabora le paghe; il medico competente in materia di igiene e sicurezza sul lavoro che effettua la sorveglianza sanitaria sui dipendenti in base al D.lgs 81/08; la società informatica che garantisce l'operatività del sistema informativo aziendale ed effettua la manutenzione dei computer.

b) Nomina a "Responsabile Esterno al Trattamento dati personali di terzi" ad una Società del Gruppo

Qualora il trattamento di dati personali sia effettuato da una Società del Gruppo per conto di committenti terzi, quest'ultimi potrebbero richiedere di designare la Società come Responsabile Esterno del trattamento dei dati personali.

Le richieste di nomina a "Responsabile Esterno al trattamento dati personali" devono essere inoltrate alla Funzione *Compliance* che provvede ad effettuare le opportune verifiche con le funzioni coinvolte nel trattamento dei dati, a restituirla firmata e a registrare la nomina ricevuta sul Registro Trattamento Dati.

6.4 Autorizzato di I Livello e Sub Responsabile Esterno

Il GDPR ha introdotto la figura del Sub-Responsabile al fine di rendere più agevole la ripartizione dei ruoli, tenendo in considerazione la pluralità di soggetti che possono intervenire nello svolgimento di un determinato servizio. Anche la figura del Sub-Responsabile può essere interna (Autorizzato di I Livello) o esterna alla Società.

Autorizzato di I Livello

Ogni Designato nell'ambito della propria Funzione ed in relazione alla complessità della struttura e/o dei trattamenti di competenza, può decidere di delegare – in tutto o in parte – le proprie funzioni ad uno o più soggetti individuati nei suoi diretti riporti (cd. "n-2"), i quali verranno nominati "Autorizzati di I Livello al Trattamento dati Personali" rispetto al Designato

La lettera di nomina a Autorizzato di I Livello al trattamento viene redatta, su indicazione del Designato , dalla Funzione Compliance.

Sub-Responsabile Esterno

Ogni Responsabile Esterno, nel caso in cui affidi i dati personali del proprio Cliente ad una terza parte, ha l'obbligo di nominare quest'ultima quale Sub-Responsabile Esterno al trattamento dati personali nell'ambito delle attività svolte. La nomina:

- nel caso in cui sia indirizzata alla Società, deve essere inoltrata alla Funzione Compliance che ne prende visione, la sottopone alla firma del Responsabile Interno di riferimento e la registra sul Registro Privacy del Gruppo Sirti;
- nel caso in cui sia la Società a dover nominare una terza parte Sub-Responsabile Esterno, per il tramite della Funzione Procurement & Supply Chain, la Società provvede ad inviare al terzo il suddetto atto che deve essere restituito compilato e firmato alla casella di posta elettronica privacy@sirti.it; una volta ricevuto controfirmato, la Funzione Compliance effettua una valutazione nel merito dell'atto e provvede alla finalizzazione del documento e alla relativa registrazione, debitamente firmato dalle parti, nell'apposito Registro Trattamento Dati.

6.5 Costituzione, pubblicazione, aggiornamento e consultazione degli elenchi dei Designati/Autorizzati e Responsabili/Sub-Responsabili del trattamento

L'elenco dei Designati/Autorizzati di I Livello della Società è consultabile sia sull'home page della intranet aziendale sia alla sezione "Compliance – Privacy" del ServiceMe aziendale sia all'interno del documento "Organigramma Privacy Gruppo Sirti".

L'elenco dei Responsabili/Sub-Responsabili Esterni è invece consultabile alla sezione "Compliance – Privacy" del ServiceMe aziendale all'interno del Registro Privacy del Gruppo Sirti.

6.5 Persona Autorizzata di II Livello

La Persona Autorizzata al trattamento dei dati è La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali e la quale compie materialmente le operazioni di trattamento.

Il Titolare ha l'obbligo di individuare come "Autorizzati di II Livello" tutte le **persone fisiche** autorizzate ad effettuare materialmente il medesimo trattamento.

Ogni Società del Gruppo Sirti ha provveduto ad individuare gli "Autorizzati di II livello al trattamento dei dati personali" nelle persone fisiche dei propri dipendenti in ragione del rapporto di lavoro intercorrente tra Titolare/Datore di Lavoro ed il Dipendente/Autorizzato.

6.5.1 Nomina della Persona Autorizzata di II Livello al trattamento dei dati - Competenze e responsabilità

Possono essere nominate Persone Autorizzate di II Livello al trattamento i dipendenti della Società, ivi inclusi quelli a tempo determinato e gli altri lavoratori (es. lavoratori "somministrati", lavoratori a progetto, stagisti).

Il personale Autorizzato è tenuto:

- a trattare i dati personali e/o riconducibili alle categorie particolari di dati personali in modo lecito e secondo correttezza;
- raccoglierli e registrarli per gli scopi inerenti l'attività svolta da ciascuno;
- verificare, ove possibile che siano esatti e, se necessario, aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare del trattamento, dal Responsabile del trattamento ovvero dal Sub-responsabile del trattamento;
- conservarli, rispettando le misure di sicurezza previste nelle Policy
- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- attenersi scrupolosamente alle procedure aziendali e alle istruzioni scritte e verbali impartite dai Responsabili e dai Sub-responsabili;
- non divulgare a terzi estranei le informazioni di cui viene a conoscenza;
- non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile o del Sub-responsabile;
- non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati, al fine di prevenire eventuali azioni fraudolente da parte di terzi;
- non lasciare incustoditi e accessibili a terzi i dispositivi utilizzati per il trattamento dei dati;
- informare tempestivamente il Responsabile o il Sub-responsabile in caso di incidenti relativi alla sicurezza sui dati;
- astenersi dal comunicare a terzi (anche se Suoi colleghi o comunque appartenenti alla struttura) in qualsiasi forma, le proprie credenziali di autenticazione, necessarie per il trattamento dei dati personali con strumenti elettronici, fatto salvo per il soggetto incaricato di custodire dette credenziali che avrà il compito di istruirla dettagliatamente in merito alle modalità di detta comunicazione.

6.6 Interessato

E' la *persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.*

Diritti dell'Interessato

L'Interessato ha sempre il diritto d'accesso ai propri dati personali detenuti dal Titolare.
Inoltre, ha sempre il diritto di conoscere quali dati personali il Titolare possiede sul proprio conto, il diritto di controllare tali dati, il diritto di opporsi al trattamento, in tutto o in parte.

Più in dettaglio, l'interessato ha diritto ad ottenere le seguenti informazioni:
- dell'esistenza di dati personali che lo riguardano,
- dell'origine dei dati personali,
- delle finalità e modalità di trattamento,
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici,
- gli estremi identificativi del titolare e dei responsabili al trattamento, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati.

Tali diritti possono essere esercitati con richiesta rivolta senza alcuna formalità al Titolare o Responsabile del trattamento.
Il Titolare del trattamento, una volta interpellato, non può omettere o rifiutarsi di fornire risposte; risposte che dovranno essere comunicate all'interessato senza ritardo.

6.7 Amministratore di sistema (Ads)

Il trattamento di dati personali effettuato con strumenti elettronici viene regolamentato dal provvedimento del Garante del 27 novembre 2008 "*Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema*".

Il termine Amministratore di Sistema (AdS) si riferisce ad una "*figura professionale, individuata nell'ambito degli Autorizzati al Trattamento, dedicata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e a tutte quelle figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati*". Ci si riferisce a titolo esemplificativo a:

- amministratori di basi di dati;
- amministratori di reti e di apparati di sicurezza;
- amministratori di sistemi software complessi;
- sviluppatori/manutentori SW;
- configuratori/manutentori HW;
- gestori di reti.

6.7.1 Nomina e competenze degli Ads

La designazione ad Amministratore di Sistema è individuale.

La designazione deve essere effettuata per iscritto dal proprio Responsabile di Funzione utilizzando il **Mod. 502029** "*Designazione ad "Amministratore di Sistema" ai sensi del provvedimento del Garante per la protezione dei dati personali del 27/11/2008 pubblicato in Gazzetta Ufficiale n. 300 del 24/12/2008*"
Il modulo – una volta compilato e debitamente firmato - deve essere inviato alla Funzione Compliance che effettua le registrazioni nel sistema informativo.

Parallelamente è necessario inviare comunicazione dell'avvenuta nuova nomina a Security Management che provvede all'aggiornamento del sistema di Log Collection.

- L'elenco completo degli Amministratori di Sistema è consultabile: *per tutte le società del Gruppo Sirti- eccetto Wellcomm Engineering- dal report* ***PGL050*** *– Amministratori di Sistema - disponibile sul portale Intranet Sirti > Report e Analisi > Personale > Anagrafiche;*

- *per il personale Wellcomm Engineering, dal report "Elenco AdS Wellcomm Engineering" disponibile presso la Funzione Compliance*

Qualora l'attività degli Amministratori di Sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, il Titolare è tenuto a rendere nota o conoscibile l'identità degli AdS nell'ambito delle propria organizzazione, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.
Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il Titolare o il Responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

La particolare attività svolta dagli Amministratori di Sistema, comporta l'adozione di una articolata serie di misure di carattere organizzativo e tecnico, di seguito elencate:

➢ l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e 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.

In particolare, devono essere valutate le **caratteristiche soggettive**:

- Affidabilità del soggetto
- Assenza di provvedimenti disciplinari attinenti privacy/security.
- Assenza di imputazioni o condanne per reati informatici di cui alla Parte Speciale del Modello di Organizzazione e Gestione (MOG), sezione "Reati di criminalità informatica e trattamento illecito di dati".

e le **competenze tecniche**, a titolo esemplificativo possono costituire elementi di valutazione:

- Specifiche certificazioni negli ambiti tecnologici ai quali è destinato ad operare
- Attestati di partecipazioni a corsi (prima di essere nominato, l'Amministratore di Sistema deve obbligatoriamente frequentare corso specifico di formazione in materia di Ads)
- Curriculum vitae
- Referenze
- Comprovata esperienza maturata

➢ l'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Responsabili di Funzione, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

➢ devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica), ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Servizi erogati a una Società del Gruppo Sirti

In caso di affidamento di attività in *outsourcing*, per le quali è previsto l'incarico di AdS, la Società nomina il fornitore Responsabile Esterno del Trattamento dei dati e detta le direttive in qualità di Titolare. Gli Amministratori di Sistema vengono designati dal fornitore che è tenuto ad aggiornare l'elenco degli AdS e a fornirlo alla Società e alle autorità se richiesto.

Nel caso di affidamento di attività in outsourcing a consulenti con partita IVA, la Società effettua direttamente la designazione del consulente ad AdS.

Servizi erogati da una Società del Gruppo Sirti

I dipendenti della Società che operano su sistemi di terze parti *in house* o presso terzi vengono designati AdS dal Responsabile di Funzione a cui fanno capo.
I dipendenti di terze parti che operano per conto della Società presso terzi (subappalto) sottostanno alle regole di cui al punto precedente (Servizi erogati a una Società del Gruppo Sirti).

6.7.2 Revoca nomina Ads

Il venir meno dei requisiti previsti per la nomina comporta la revoca senza indugio della designazione e la conseguente cancellazione dei diritti di accesso ai sistemi precedentemente amministrati.
Altri eventi che possono determinare variazioni alla designazione sono:

- Cambio di qualifica (modifica designazione). Se i sistemi su cui andrà ad operare il dipendente contengono anch'essi dati tutelati, il Responsabile di Funzione provvede ad emettere nuova designazione.
- Assenza prolungata (sospensione designazione). In caso di prolungata assenza dell'AdS il Responsabile di Funzione provvede a far disabilitare l'utenza e ad effettuare la sospensione della designazione ad AdS.
- Altro (revoca designazione).

In tutti i casi elencati sopra, il modulo di revoca viene inoltrato alla Funzione Compliance la quale provvede ad aggiornare il sistema informativo aziendale ed alla Funzione Security Management che, dopo le verifiche necessarie, provvede all'aggiornamento del Sistema di Log Collection. Per la società Wellcomm il modello viene inoltrato alla Funzione IT Office per Wellcomm Engineering)

La **revoca** deve essere formalizzata utilizzando il modulo n. **504896** disponibile nel sistema documentale Vista Plus > Normativa > Moduli.

6.7.3 Compiti e responsabilità dell'Amministratore di Sistema

I principali compiti e responsabilità che competono ad un AdS sono:

- gestire il sistema informatico, nel quale risiedono le banche dati personali, in osservanza delle misure di sicurezza disposte dal Titolare e/o del Responsabile secondo quanto previsto dalla normativa vigente in materia di privacy
- monitorare il sistema di sicurezza informatico adottato (idoneo a rispettare il Disciplinare Tecnico), adeguandolo anche alle eventuali future norme in materia di sicurezza. Più specificatamente, in base al sopra citato vigente disciplinare tecnico, fatte salve le successive integrazioni dello stesso, in qualità di Amministratore di Sistema deve:
  - gestire il sistema di autenticazione informatica (rilascio e revoca delle credenziali di accesso al sistema) secondo le modalità indicate nel Disciplinare Tecnico;
  - gestire il sistema di autorizzazione informatica (definizione, rilascio e revoca dei profili di autorizzazione per l'accesso ai dati),
  - adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a migliorare la sicurezza nel rispetto di quanto previsto dalla normativa vigente e verificando l'installazione, l'aggiornamento ed il funzionamento degli stessi,
  - adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali, provvedere al salvataggio periodico degli stessi con copie di back-up e assicurarsi della qualità delle copie di back-up e della loro conservazione in luogo adatto e sicuro;
  - indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla

luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;
- vigilare sugli interventi informatici diretti al sistema informatico della Società, effettuati da operatori esterni, e in caso di anomalie dare opportuna segnalazione al Titolare e/o al Responsabile;
- monitorare le eventuali ulteriori misure minime di sicurezza imposte dal Disciplinare Tecnico per il trattamento informatico dei dati sensibili e giudiziari e per la conseguente tutela degli strumenti elettronici utilizzati per il trattamento;

- collaborare con il Titolare e/o con il Responsabile per l'attuazione delle prescrizioni impartite dal Garante;
- comunicare prontamente al Titolare e/o al Responsabile qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
- verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati sui PC, riferendo al Titolare e/o al Responsabile.

6.8 Funzione Compliance

La Funzione *Compliance*, in qualità di "Referente Privacy" di Gruppo, si occupa della gestione di tutte le tematiche inerenti l'adeguatezza dei processi aziendali alla normativa vigente in materia di privacy prestando supporto al Titolare del trattamento ed al DPO.

Fornisce supporto, collaborando con i Responsabili ed i Designati, per l'attuazione delle disposizioni di legge e la loro interpretazione.

Compiti e responsabilità

Alla Funzione *Compliance* è attribuita la responsabilità del presidio interno della normativa, del coordinamento e monitoraggio in materia di privacy.

I principali compiti attribuiti alla Funzione *Compliance* sono:

- supportare il DPO in tutte le sue attività di:
    - consulenza al Titolare, al Responsabile nonché ai dipendenti che eseguono attività di trattamento dati personali in merito agli obblighi derivanti dalla normativa vigente in materia di privacy;
    - sorvegliare l'osservanza della normativa vigente in materia di privacy, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
    - fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR;
    - cooperare con il Garante per la protezione dei dati personali;
    - ogni altro compito connesso a quanto sopra, anche in virtù di disposizioni di legge o contenute in provvedimenti del Garante per la protezione dei dati personali.

- coordinare tutte le attività e gli adempimenti in materia per il supporto tecnico-giuridico in caso di dubbi interpretativi sulle vigenti disposizioni di legge e sulle procedure aziendali, nonché per risolvere eventuali criticità riscontrate con i controlli interni;

- realizzare il sistema di controllo al fine di dare attuazione all'obbligo di vigilanza che la legge pone in capo al Titolare del trattamento;

- garantire la diffusione e la corretta applicazione della presente policy e delle altre procedure correlate all'interno della Società assicurando in tutti i casi la necessaria assistenza e supporto operativo;

- svolgere attività di supporto e sensibilizzazione dei Responsabili e degli Incaricati circa la necessità di attenersi alle disposizioni in materia di trattamento dei dati personali, anche attraverso incontri *ad hoc* e/o corsi di formazione specifici

- collaborare con il DPO, con la Funzione Security Management per gli aspetti più specifici di sicurezza informatica e con le altre funzioni aziendali interessate e coinvolte in materia di privacy.

7. DISPOSIZIONI GENERALI SUL TRATTAMENTO DEI DATI

Nel seguito sono riportati i principi e le disposizioni generali applicabili ai trattamenti effettuati dalla Società sui dati personali di tutte le categorie di interessati (dipendenti, clienti, azionisti, ecc.), tenendo presente che i dati personali oggetto di trattamento devono essere:

- trattati in **modo lecito, corretto e trasparente** nei confronti dell'interessato nel rispetto delle norme del GDPR

ad esempio, previa informativa e, ove necessario, con il consenso dell'interessato;

- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi

ad esempio, non possono essere raccolti dati personali in attesa di decidere quando e come utilizzarli, così come non possono essere utilizzati per scopi diversi da quelli per i quali sono stati raccolti;

- **esatti** e, se necessario, aggiornati

ad esempio, aggiornandoli secondo le comunicazioni degli interessati, come nel caso dell'aggiornamento del titolo di studio dei dipendenti, anche se conseguito successivamente all'assunzione, sul quale cfr. anche Newsletter del Garante del 6 gennaio 2003

- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati. Ciò significa che nelle operazioni di trattamento non devono essere utilizzati i dati che non siano strettamente necessari per tali operazioni.

ad esempio, nel predisporre l'elenco di dipendenti che hanno partecipato ad un corso di formazione non dovranno essere indicati date di nascita, codici fiscali, ed ogni altro dato personale, se non sono effettivamente necessari alle finalità di tale elenco

- **conservati** in una forma che consenta l'identificazione dell'interessato e per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (vedi tempo di conservazione dati indicato nel Registro Trattamento Dati Personali del Gruppo Sirti).

ad esempio, non oltre il tempo impiegato per fornire all'interessato una certa prestazione richiesta o per svolgere una determinata attività prevista dal contratto con il cliente e riportato nel Registro Trattamento

- utilizzati secondo il principio di **necessità** e secondo le **finalità del trattamento** individuate**,** che presuppone la configurazione dei sistemi informativi e dei *software* in modo tale da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità consentite.

ad esempio, predisponendo o aggiornando i software in modo tale da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi

- **custoditi e controllati**, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi, anche accidentali, di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Sulla base di quanto sopra, con particolare riferimento alla "comunicazione" o scambio dei dati personali nell'ambito delle attività lavorative, si precisa che:

- ogni Funzione o soggetto può trattare solo i dati personali di competenza, necessari per il conseguimento delle rispettive finalità **("*need to know*");**

se per effettuare una certa operazione per i clienti è sufficiente conoscere solo il numero telefonico, tutti gli altri dati personali come il nome, il codice fiscale, ecc., non devono essere utilizzati o comunicati ad altre funzioni/soggetti.

- i dati personali **non** devono essere messi a disposizione/conoscenza di Funzioni/soggetti che non abbiano la necessità lavorativa di venirne a conoscenza. Ovviamente, questo principio non si applica se i dati oggetto di comunicazione o scambio sono in forma anonima o aggregata in modo non riconducibile a singole persone o soggetti identificati od identificabili;

- quando non è possibile utilizzare dati anonimi o aggregati in modo non riconducibile a singole persone o soggetti identificati od identificabili, l'impiego di dati personali deve essere il più limitato possibile.

7.1 Ulteriori principi e disposizioni generali per la conservazione dei dati

I dati personali devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

La conservazione dei dati personali può essere affidata anche a soggetti terzi, tramite appositi contratti che, in ottemperanza alle disposizioni di legge vigenti, disciplinino dettagliatamente le modalità ed i tempi di conservazione e che prevedano la nomina a Responsabile Esterno del trattamento.

Il principio di esattezza del dato personale
Secondo il "principio di esattezza del dato personale" stabilito dal GDPR, il dato personale deve essere "*esatto e, se necessario, aggiornato: devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*".

7.2 Principali adempimenti correlati al trattamento dei dati personali

Nel seguito sono descritti i principali adempimenti in materia di trattamento di dati personali che devono essere assolti dalla Società.
La loro disciplina è essenzialmente di carattere generale ed è applicabile a qualsiasi categoria di interessato (dipendenti, clienti, fornitori, azionisti, ecc.) cui i dati trattati si riferiscono.

Informativa

Tutte le persone fisiche di cui vengono trattati dati personali a qualunque titolo, vanno Informate circa il trattamento, ai sensi dell'art. 13 del Regolamento EU 2016/679 (GDPR).

L'informativa è l'insieme delle informazioni di seguito riportate, che i Titolari devono fornire agli interessati (clienti, dipendenti, fornitori, visitatori) al momento della raccolta dei dati:

- le finalità e le modalità del trattamento che si intende effettuare;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di conferire i dati o dell'eventuale consenso al trattamento;
- l'indicazione dei diritti che l'interessato può esercitare in relazione al trattamento dei suoi dati (accesso, modifica, cancellazione, ecc.);
- la denominazione sociale e l'indirizzo del Titolare;
- l'eventuale ambito di comunicazione e diffusione dei dati;
- l'indicazione dei soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati del trattamento;

- i riferimenti di almeno un Responsabile del trattamento, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco nominativo aggiornato dei Responsabili (interni e terzi).

L'informativa deve essere sempre resa agli interessati, per iscritto, all'atto della raccolta dei dati, anche quando non è necessario richiedere il loro consenso al trattamento.

Sulla base di quanto sopra, ne derivano i seguenti principali **divieti** relativi all'informativa:

- **Non** è consentito effettuare trattamenti di dati personali senza aver fornito preventivamente l'informativa;
- **Non** è consentito effettuare trattamenti di dati personali per finalità diverse da quelle indicate nell'informativa già resa agli interessati; ulteriori finalità possono essere integrate previa condivisione con la Funzione *Compliance* di competenza;
- **Non** è consentita la comunicazione dei dati alle categorie dei soggetti terzi diverse da quelle indicate nell'informativa.

Consenso

Per consenso si intende l'autorizzazione che l'interessato fornisce liberamente (al Titolare) per il trattamento dei propri dati personali.

Il consenso è validamente prestato esclusivamente se:

- è espresso liberamente, preventivamente e specificamente in riferimento ad ogni singolo trattamento chiaramente individuato;
- è fornito per iscritto o è documentato per iscritto (cioè annotando e conservando tutti i riferimenti relativi all'interessato ed alla persona che lo riceve, alla data ed al luogo di ricevimento, all'oggetto delle attività/servizi per i quali viene richiesto, in allegato alla copia dell'informativa);
- è valido anche se espresso tramite *Web* (ad esempio, tramite apposizione di un *flag*, su un campo obbligatorio, in segno di autorizzazione al trattamento, prima dell'invio dell'adesione), purché rimanga un'evidenza dell'operazione, del testo visualizzato dall'utente;
- è fornito esclusivamente per iscritto in caso di dati particolari. Quando il consenso per i dati particolari è manifestato a mezzo Web è valido solo se sottoscritto con firma digitale e sono rispettati i principi e gli accorgimenti sopra richiamati;
- è stata resa l'informativa all'interessato.

L'interessato (cliente, dipendente, ecc.) può in qualsiasi momento revocare il consenso in precedenza manifestato, così come può in qualsiasi momento manifestare il proprio consenso in precedenza negato.

Il consenso per il trattamento non è richiesto quando il trattamento medesimo viene effettuato secondo una delle seguenti basi giuridiche (art. 6 GDPR):

- adempimento di obblighi contrattuali o di misure precontrattuali
- obblighi di legge cui è soggetto il Titolare del trattamento
- interessi vitali della persona interessata o di terzi
- legittimo interesse prevalente del Titolare o di terzi cui i dati vengono comunicati
- interesse pubblico o esercizio di pubblici poteri

8. TRATTAMENTO DEI DATI PERSONALI NEL PROCESSO DI HR MANAGEMENT

Nel presente paragrafo vengono riportate le modalità di trattamento dei dati nelle varie fasi del processo di HR Management.

A) Pubblicazione Annunci di lavoro

Gli annunci di lavoro richiedono una chiara Informativa che permetta all'Interessato di comprendere i seguenti aspetti:

- L'identità del Titolare del trattamento dei dati riportati nei curricula e le finalità e modalità del trattamento, specificando se vi sono ulteriori finalità oltre quelle connesse alla specifica ricerca del personale. Devono essere indicati anche i tempi di conservazione.
- L'eventualità che i dati siano divulgati a terzi

B) Curriculum

- Nel caso in cui sia l'Interessato a inoltrare alla Società l'autocandidatura o a rispondere ad un annuncio presente sul sito internet aziendale, il candidato sarà obbligato a prendere visione dell'Informativa sul trattamento dei dati personali prima di poter concludere il processo di caricamento del proprio CV.

- Nel caso in cui sia la Società ad avviare un processo di selezione del personale, i candidati saranno invitati a caricare i CV sul portale aziendale in modo da dover prendere visione dell'Informativa sulla privacy e ad esprimere il loro consenso.

Al candidato che viene selezionato per l'assunzione deve essere sottoposta preventivamente l'Informativa privacy resa ai sensi dell'art.13 del GDPR necessaria per la gestione del rapporto di lavoro.

C) Il trattamento dei dati personali per la valutazione di attitudini o profili professionali

Secondo i principi affermati dal D.Lgs. 101/2018 e dalle normative in ambito giuslavoristico (art. 8 dello Statuto dei lavoratori, art. 10 del D.Lgs 276/2003 o c.d. Legge Biagi), nelle attività di reclutamento dei lavoratori i dati personali necessari per la valutazione delle attitudini professionali dei candidati e del loro inserimento lavorativo, devono essere raccolti ponendo particolare attenzione ad evitare qualsiasi trattamento discriminatorio od indagine su caratteristiche che non incidono sulle modalità di svolgimento dell'attività lavorativa.

Il trattamento dei dati dei lavoratori mediante l'impiego di test psicoattitudinali o procedure di valutazione del suo carattere o personalità è effettuato previo consenso del candidato o lavoratore interessato.
Ogni lavoratore ha la facoltà di conoscere i risultati di eventuali test o analisi effettuati sulla sua persona (ad esempio, per l'assunzione, avanzamento di carriera, attribuzione di premi) e il diritto di essere informato sull'esistenza di un eventuale trattamento automatizzato dei suoi dati personali diretto a definirne il carattere, profilo o personalità.

D) Trattamento dei dati sanitari dei lavoratori

E' vietata qualsiasi forma di diffusione dei dati sanitari dei lavoratori (tramite pubblicazione, ad es.su bacheche o pagine web consultabili da chiunque).

E' vietata la pubblicazione di qualsiasi informazione da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Le cartelle sanitarie dei dipendenti vengono conservate separatamente da ogni altro dato personale dell'interessato, anche con riferimento ai fascicoli personali cartacei dei dipendenti.

E) Trattamento dei dati sanitari dei lavoratori in materia di sicurezza sul lavoro (D.lgs 81/08)

Il Datore di Lavoro non può accedere alle cartelle sanitarie e di rischio, ma è tenuto ad assicurarne un'efficace custodia (anche ai fini di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti).

Il Datore di Lavoro non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente (dal punto di vista sanitario) allo svolgimento di date mansioni, sebbene sia tenuto, su parere del medico competente (o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati.

Al riguardo il Medico Competente, sulla base delle risultanze delle visite mediche, può esprimere uno dei seguenti giudizi relativi alla mansione specifica: a) idoneità; b) idoneità parziale con prescrizioni o limitazioni; c) inidoneità temporanea; d) inidoneità permanente.

Per quanto riguarda in particolare la gestione/conservazione delle cartelle sanitarie e di rischio dei lavoratori si rinvia alla procedura 500836 sez. 3 "Gestione della sicurezza sul lavoro – visite mediche".

Il Medico Competente si configura come Titolare Autonomo nei confronti del trattamento dei dati sanitari dei dipendenti delle Società del Gruppo.

9. ACCESSO ALLE SEDI - TRATTAMENTO DEI DATI PERSONALI DEI VISITATORI PRESSO LE SEDI AZIENDALI

9.1 Trattamento dei dati personali presso le sedi con servizio di vigilanza e/o reception

Il trattamento dei dati personali (nome, cognome, data di nascita ed estremi del documento di riconoscimento) dei terzi che accedono ai siti aziendali (visitatori occasionali o pubblico in generale) è consentito solo **previa Informativa** agli interessati.

L'Informativa deve essere consegnata al visitatore all'ingresso di ogni sede prima della registrazione dello stesso.

L'Istituto di Vigilanza/Reception che effettua il trattamento dei dati, deve essere nominato Responsabile Esterno del trattamento.

10. VIDEOSORVEGLIANZA - TRATTAMENTO DEI DATI PERSONALI DEI VISITATORI PRESSO LE SEDI AZIENDALI

La presente disciplina si applica in tutti i casi in cui vengono utilizzate telecamere per riprendere e registrare immagini e suoni presso le sedi aziendali, ed in particolare quando le telecamere sono installate in prossimità dei varchi di accesso, lungo il perimetro e all'interno delle sedi per motivi di tutela del patrimonio aziendale.
E' opportuno precisare che la normativa privacy (in particolare il Provvedimento del Garante Privacy in materia di videosorveglianza del 8 aprile 2010 e le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video) e quella giuslavoristica (in particolare, l'art. 4 della legge 300/1970) consentono ad un soggetto privato di utilizzare la videosorveglianza esclusivamente per ragioni di protezione delle persone, della proprietà o del patrimonio, nel rispetto nelle disposizioni di seguito riportate.

L'utilizzo di dispositivi di raccolta, gestione e conservazione di suoni e immagini, è consentito a condizione che siano fornite adeguate informazioni all'interessato circa la possibilità di essere ripreso dalle telecamere e che, oltre alle disposizioni di carattere generale previste dalla normativa vigente in materia di trattamento dei dati personali, siano osservate le seguenti ulteriori specifiche indicazioni, tratte dal provvedimento del Garante del 08 aprile 2010 (Provvedimento in materia di videosorveglianza):

- il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi. Ciò comporta che il Titolare può perseguire solo finalità di sua pertinenza;

- è necessario fornire indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza; è necessario, inoltre, fornire l'informativa ai sensi dell'articolo 13 del GDPR tramite affissione all'ingresso o alla reception della società.

- occorre rispettare il principio di necessità, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
  Il sistema informativo ed il relativo programma informatico devono essere conformati in origine in modo tale da non utilizzare impiegando solo dati anonimi.

- il software va configurato in modo da cancellare periodicamente ed automaticamente i dati eventualmente registrati. Quando è necessario conservare i dati, il periodo di conservazione delle immagini deve essere limitato al massimo alle 24 ore successive alla rilevazione, fatta eccezione per esigenze di chiusura per festività o chiusura di uffici e per esigenze investigative dell'Autorità Giudiziaria; un eventuale allungamento dei tempi di conservazione (non superiore comunque ad una settimana) deve essere motivato da esigenze eccezionali.

- il Titolare è tenuto ad effettuare un costante monitoraggio per assicurare che la conservazione dei dati registrati avvenga effettivamente entro il periodo massimo di 24 ore. In relazione alle esigenze eccezionali indicate dal Garante Privacy nel suddetto provvedimento e di cui si è fatto cenno sopra, si precisa quanto segue: le esigenze di una conservazione oltre le 24 ore delle immagini registrate potrebbero derivare, ad esempio, a seguito di un evento criminoso già accaduto (attentati, danneggiamenti ripetuti, ecc.) o realmente incombente, oppure in relazione alla necessità di custodire o consegnare una copia delle registrazioni richieste dall'Autorità Giudiziaria (a seguito di denunce presentate dalle Società).

- La conservazione deve essere limitata al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria o per tutela del patrimonio aziendale in caso di rischio elevato per il perpetrarsi di eventi criminosi effettivamente accaduti, adeguatamente documentati (es. filmati, denunce di furto e/o altro, segnalazioni interne, etc.) e per porre in esser azioni a tutela dei dipendenti stessi.

11. SANZIONI

L'art. 83 del Reg. UE 2016/679 ha introdotto i seguenti due livelli di sanzioni amministrative pecuniarie:

- L'art 83 comma 4 prevede fino a 10.000,00 euro di sanzione, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente;

- L'art 83 comma 5 prevede sanzioni amministrative pecuniarie fino a 20.000,00 euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente

definendo altresì le diverse fattispecie sanzionabili.

Il D.Lgs 101/2018, che ha modificato il Codice Privacy allo scopo di adeguarlo al nuovo assetto legislativo introdotto dal GDPR, ha - a sua volta - identificato altre fattispecie la cui violazione comporterà l'applicazione delle sanzioni di cui sopra (art. 166 del nuovo Codice Privacy oggi vigente).

Inoltre lo stesso Decreto 101 ha modificato il Codice Privacy introducendo nuove fattispecie sanzionate penalmente (artt. 167-172). Le fattispecie per cui saranno applicabili sanzioni penali sono quindi, ai sensi del riformato Codice Privacy, le seguenti:

Art. 167 - Trattamento illecito dei dati;
Art. 167-bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
Art. 167-ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;
Art. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
Art. 170 - Inosservanza dei provvedimenti del Garante;

GESTIONE CASELLA DI POSTA ELETTRONICA

La posta elettronica è lo strumento di comunicazione principale in azienda utilizzato sia verso clienti interni che esterni.

Come definito nella Policy n. 508358 "Information Security" adottata dalla Società, la casella di posta elettronica aziendale può essere individuale o condivisa e viene rilasciata solo agli utenti che ne hanno necessità per lo svolgimento dell'attività lavorativa e solo previa richiesta da parte del Responsabile Organizzativo o di persona delegata.

Con particolare riferimento alla casella di posta elettronica individuale si segnala che, pur essendo i domini aziendali "@sirti.it" e "wellcomm.it", gli stessi risultano essere un dato personale del dipendente. Trattandosi di strumento aziendale, il cui utilizzo è consentito solo per finalità connesse allo svolgimento dell'attività lavorativa, la casella di posta elettronica non deve essere utilizzata per comunicazioni personali.

È infatti necessario essere consapevoli del fatto che, in particolari condizioni, la legge consente al Datore di Lavoro di accedere alla casella di posta del lavoratore per:

- assicurare la continuità operativa dell'azienda, avendo accesso ad informazioni o documentazione di particolare rilevanza per la Società, presenti nell'email del dipendente (assente per qualche motivo o il cui rapporto di lavoro sia giunto al termine);
- utilizzare delle e-mail presenti nella casella di posta del lavoratore per fini disciplinari.

Alla cessazione del rapporto di lavoro, l'accesso alla casella di posta viene inibito immediatamente alla chiusura dell'account e la casella viene sospesa impedendo in tal modo l'invio e la ricezione della posta. La casella viene chiusa definitivamente dopo 30gg. Il tempo di conservazione dei messaggi di posta elettronica varia invece a seconda dell'attività svolta dal dipendente; all'interno del Registro Privacy o nella

sezione Compliance – Privacy del ServiceMe aziendale è possibile consultare l'elenco riportante l'associazione mansione/tempo di conservazione della posta elettronica.