Modello Organizzativo

Trattamento Dati Personali

GDPR PRIVACY POLICY

REGOLAMENTO 679:2016

Revisione	Data	Classificazione	Preparato da:	Approvato da:	Firma
00	01-01-2022	PRIVACY POLICY	DANIELE BALANI	TITOLARE DEL TRATTAMENTO **DANIELE BALANI**	
				DPO [DATA PROTECTION OFFICER] **DANIELE BALANI**	

Tracciabilità delle revisioni		
Revisione	**Data**	**Descrizione**
00	01-01-2022	PRIMA EMISSIONE

NOME AZIENDA	INDIRIZZO – Sede Centrale	PARTITA IVA
FLASH LINE MAINTENANCE S.R.L.	VIA PASSO BUOLE 97 BC FIUMICINO	14546711004

MODELLO ORGANIZZATIVO
TRATTAMENTO DATI
GDPR – PRIVACY POLICY
Versione 1.0
Data: 01-01-2022

1. Introduzione e contesto.

Il legislatore europeo ha deciso di rinnovare la normativa in essere in materia di trattamento dati personali (Direttiva 95/46/EC), vecchia di ormai più di vent'anni, per adeguarla all'attuale contesto tecnologico e sociale fortemente "data-centrico": ha così emanato il Regolamento (UE) 2016/679 del Parlamento e del Concilio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il GDPR è direttamente applicabile in tutti gli stati membri dell'Unione a far data dal 25 maggio 2018, essendo stato adottato con la formula del Regolamento Europeo; il GDPR persegue lo scopo di armonizzare la disciplina degli stati membri in materia di trattamento dati personali, adeguandola al contesto digitale ed introducendo quella che può a ragione definirsi la normativa di protezione dei dati più severa al mondo, capace anche di effetti extra-territoriali.

Con il GDPR la protezione dei dati personali diventa un diritto fondamentale dell'individuo, che si intende garantire obbligando chi effettua trattamenti ad adeguarsi ai principi di Privacy "by design" e "by default".

In linea con i principi di cui sopra, il GDPR pone l'accento sulle caratteristiche di trasparenza e rendicontazione richieste ai trattamenti effettuati sui dati personali, prevedendo la necessità di dimostrare il rispetto dei trattamenti effettuati alle previsioni normative.

Pertanto, il GDPR impone nuovi obblighi a società, enti governativi, organizzazione e associazioni non-profit che offrono beni e servizi ai cittadini europei o che, comunque, nell'esercizio della propria attività raccolgono e trattano dati riferibili a persone fisiche.

Alla luce di quanto sopra e traendo vantaggio dalla raggiunta armonizzazione della normativa a livello europeo, FLASH LINE MAINTENANCE S.R.L. ha deciso di adottare il presente Modello Organizzativo Trattamento Dati Personali, al fine di garantire il rispetto di quanto previsto dal GDPR e dare piena efficacia ai principi di privacy by design e by default.

2. Definizioni

Nel presente Modello Organizzativo Trattamento Dati Personali i termini qui elencati assumo i seguenti significati:

Autorità di Controllo	Autorità pubblica incaricate di sorvegliare l'applicazione del GDPR; l'elenco delle Autorità competenti per paese è qui allegato quale.
Dato Personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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 relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi fi assistenza sanitaria, che rivelano informazioni al suo stato di salute (vedi considerando 35)
* Considerando 35	Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.
GDPR	Regolamento (UE) 2016/679 del Parlamento e del Consilio Europeo
MOTDP	Il presente Modello Organizzativo Trattamento Dati Personali
Responsabile del Trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta o sotto la cui responsabilità e controllo vengono trattati dati personali per conto del Titolare.
Titolare	Legale rappresentate della Società che determina le finalità e i mezzi del trattamento di dati personali;
Trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica,

l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

3. Scopo

L'adozione del presente Modello Organizzativo Trattamento Dati Personali è finalizzata a garantire il rispetto di ogni obbligo di legge posto a carico del Titolare del Trattamento di **FLASH LINE MAINTENANCE S.R.L.** ed in particolare:

1. Definisce un modello organizzativo finalizzato ad una efficace ed uniforme gestione dei Trattamenti all'interno della società;
2. Assicura agli interessati (dipendenti, clienti, fornitori, consulenti e terzi) la liceità dei Trattamenti dei Dati che li riguardano, nonché la possibilità di esercitare i diritti loro garantiti dal GDPR;
3. Assicura che a protezione dei Dati sia garantita fin dalla progettazione dei flussi che descrivono i Trattamenti e che le misure di protezione dei Dati vengano applicate come impostazione predefinita;
4. Istituisce una procedura per l'analisi dei trattamenti fornendo ai Titolari e ai responsabili individuati gli strumenti e i criteri per la costituzione del Registro dei Trattamenti;
5. Individua le misure di sicurezza informatica implementate in**FLASH LINE MAINTENANCE S.R.L.** per garantire la sicurezza dei Dati.

4. Ambito d'Applicazione

Il presente MOTDP è vincolante per **FLASH LINE MAINTENANCE S.R.L.** attraverso il suo Titolare del Trattamento, che si impegna a adottarlo, anche ai sensi dell'art. 47 GDPR, sottoscrivendo le lettere di adesione di cui al modulo 000.

Gli obblighi di Trattamento assunti dal Titolare ai sensi del presente MOTDP sono vincolanti anche nei confronti degli interessati o eventuali responsabili interni ed esterni.

5. Titolari del Trattamento

Il TITOLARE DEL TRATTAMENTO determina le finalità dei trattamenti dei dati di **FLASH LINE MAINTENANCE S.R.L.** impegnandosi ad effettuare trattamenti in conformità al presente MOTDP ed in modo lecito, corretto e trasparente nei confronti degli interessati. Il Titolare del Trattamento garantisce nei confronti degli interessati, che:

a) I Trattamenti effettuati siano conformi alle finalità dichiarate;

b) Le finalità dichiarate siano limitate a quanto necessario per l'esercizio dell'attività del Titolare;

c) Vengano utilizzati solo i dati necessari per le finalità dichiarate;

d) La conservazione dei dati sia limitata nel tempo ad un periodo congrui con le finalità dichiarate;

e) Siano implementati sistemi atti a garantire la conservazione dei dati,

f) Per ogni Trattamento sia verificato il criterio di legittimità del Trattamento;

g) Con cadenza ogni 2 anni venga promossa una verifica del livello di Compliance alla normativa e una revisione delle Schede di Analisi dei Trattamenti e vengano definiti piani di miglioramento nella gestione dei Trattamenti;

h) Le informative rilasciate agli interessati siano conformi a quelle indicate nelle Linee Guida per la gestione dei Trattamenti e che quindi menzionino l'esistenza del presente MOTDP ed i suoi contenuti principali, nonché forniscano le informazioni necessarie per attivare la procedura descritta al successivo Articolo 14.

Alla luce dell'uniforme livello di protezione dei Dati, è consentito la trasmissione di Dati tra i Titolari a condizione che: (i) la trasmissione sia necessaria per le finalità per cui il dato è Trattato; (ii) la trasmissione sia stata compresa tra i trattamenti elencati nell'informativa rilasciata al momento della raccolta del Dato; oppure che la trasmissione sia necessaria per l'erogazione di un servizio da una società all'altra.

6. Referente Privacy / DPO [Data Protection Officer]

Valutati i criteri dettati dall'art. 37 GDPR, **FLASH LINE MAINTENANCE S.R.L.** ha provveduto alla nomina di "Responsabili della Protezione dei Dati" per le diverse funzioni aziendali.

Ciò nondimeno, al fine di garantire al Titolare del trattamento un supporto qualificato per la gestione, valutazione e aggiornamento dei requisiti previsti dal GDPR, nonché per garantire adeguati e uniformi livelli di sicurezza nel trattamento dei dati, per **FLASH LINE MAINTENANCE S.R.L.** è stata istituita la figura del "*Referente Privacy*", nella persona del ***D.P.O*** [**D**ata **P**rotection **O**fficer]

nominato formalmente mediante Mod. 014 ed come DPO, del quale si allega evidenza formativa di certificazione della competenza ai sensi della NORMA 11697:2017 (allegato 015)

Il Referente Privacy / ***D.P.O*** svolge l'attività consulenziale di ***supervisore indipendente***, a favore del Titolare e dei Responsabili del Trattamento e dietro loro richiesta.

Inoltre, ai sensi del presente MOTDP il Referente Privacy/ ***D.P.O***:

a) Viene indicato dal Titolare come punto di contatto unico per FLASH LINE MAINTENANCE S.R.L. per le richieste degli interessati;

b) Si occupa di monitorare l'evoluzione della normativa e dei provvedimenti delle Autorità di Controllo e aggiornare Titolare e Responsabili ove questi possano avere un impatto sui Trattamenti di cui al Registro dei Trattamenti;

c) Coordina le attività di analisi dei trattamenti effettuate dal Titolare e Responsabili incoraggiando un uniforme e adeguato livello di sicurezza nel trattamento dei Dati Personali;

d) Con cadenza almeno annuale, promuove e coordina con il Titolare una revisione dei contenuti delle Linee Guida per la Gestione dei Trattamenti, delle Schede di Analisi dei Trattamenti e supporta il Titolare nella definizione di piani di miglioramento;

e) Assiste il Titolare nell'erogare una appropriata formazione in materia di protezione dei Dati al personale che ha accesso permanente o regolare ai Dati;

f) Raccogliere le richieste degli Interessanti, informando il Titolare e i Responsabili coinvolti e assistendoli nell'evasione di tali richieste;

g) Mantiene il registro delle violazioni per il Titolare;

h) Se presente, rappresenta il punto di contatto con le Autorità di Controllo, assistendo il Titolare nelle relazioni con le Autorità.

7. Responsabili del Trattamento

Valutando la struttura organizzativa di FLASH LINE MAINTENANCE S.R.L. composta oltre che dalla sede centrale da Unità Operative nelle varie regioni italiane e dall'estero, il Titolare del Trattamento esercita attività di direzione e coordinamento dei processi comuni, e nomina i Responsabili del Trattamento, anche esterni.

Gli eventuali Responsabili del Trattamento (anche esterni) nominati dal Titolare dovranno:

a) garantire che le persone autorizzate al trattamento dei dati personali siano a conoscenza e vincolate a obblighi di riservatezza in relazione ai Dati che si trovano a trattare;

b) coadiuvare il Titolare nella mappatura dei trattamenti e nella redazione delle Schede di Analisi dei Trattamenti;

c) Adottare le misure di sicurezza previste dalle Schede di Analisi e dal successivo articolo 13;

d) assistere il Titolare del Trattamento segnalando la necessità di adottare misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del Trattamento di √evadere le richieste degli interessati di cancellare, modificare o restituire tutti i Dati Personali;

e) provvedere alla cancellazione o restituzione dei Dati Personali esaurita la finalità per cui sono stati raccolti e trattati.

8. Organizzazione e Responsabilità

In virtù della struttura organizzativa di **FLASH LINE MAINTENANCE S.R.L.** viene di seguito indicata la mappatura dei processi in cui Titolare e Responsabili, nonché il DPO condividono responsabilità sui singoli Trattamenti:

Tipo di trattamento	Titolare Trattamento DANIELE BALANI	Responsabile Trattamento (vedi elenco allegato 009)	Data Protection Officer (DPO)
Dati comuni e sensibili dei dipendenti	√	√	√
Gestione e trattamento Videosorveglianza (la dove implementata)	√	√	√
Dati comuni Clienti e Fornitori	√	√	
	√	√	
Profilazione dati da attività commerciale	√	√	
Trattamento e gestione dati informatici	√		
Coordinamento delle attività di analisi dei trattamenti	√		√
Verifica della conformità al trattamento dei dati	√	√	√
Mantenimento del registro delle violazioni	√	√	√
Controllare che le violazioni dei dati personali siano documentate, notificate e comunicate;			√
Audit di mantenimento sistema privacy	√		√
Attribuzione e sorveglianza di ruoli e responsabilità	√		√ (sorveglianza)
Informare e consigliare il Titolare del trattamento in merito agli obblighi derivanti dalla normativa e conservare la documentazione da questa prevista;			√

Inoltre, le attività previste per il rispetto della normativa vengono così suddivise:

Tabella Matrici di Responsabilità					
Attività	Responsabilità	Titolare Trattamento	Responsabile Trattamento	Referente Privacy / D.P.O	Responsabile IT (interno ed esterno)
Redazione delle schede di Analisi dei Trattamenti	Principale	X	X		
	Contributiva			x	
Valutazione del rischio connesso ai trattamenti	Principale	X		X	
	Contributiva		x		x
Valutazione d'impatto sulla protezione dei dati	Principale	X		X	
	Contributiva		x		
Prevedere ed implementare misure di sicurezza informatica	Principale				X
	Contributiva	X	x		
Implementare misure organizzative per la gestione dei Trattamenti	Principale	X		X	
	Contributiva		x		
Predisposizione della modulistica standard	Principale			X	
	Contributiva	x	x		
Vigilanza sul rispetto delle prescrizioni del presente MOTDP	Principale	X	X		
	Contributiva				X
Dare seguito alle richieste per l'esercizio dei diritti dell'interessato	Principale	X		X	
	Contributiva		x		
Comunicazione di una violazione dei dati personali	Principale	X		X	
	Contributiva		x		x
Formazione del personale sui GDPR e del presente MOTDP	Principale	X		X	
	Contributiva		x		
Definire piani di miglioramento e monitorarne esecuzione	Principale	X	X		
	Contributiva			x	
Rivedere periodicamente le Schede di Analisi e il livello	Principale	X	X		
	Contributiva			x	

9. Organizzazione Sede Centrale FLASH LINE MAINTENANCE e unità esterne

Nelle sedi periferiche permane quale RESPONSABILE del TRATTAMENTO il responsabile della Sede Centrale

10. Scheda di Analisi Trattamenti

Il rispetto delle previsioni del GDPR assume quale presupposto essenziale la mappatura dei trattamenti trattati.

Al fine di garantire completezza delle informazioni mappate e uniformità di analisi i Titolari e i Responsabili provvederanno a tracciare i Trattamenti effettuati mediante l'utilizzo del modello di Scheda di Analisi Trattamenti Allegato 004.

La Scheda di Analisi Trattamenti verrà compilata per ciascuna area di competenza in cui viene suddivisa l'organizzazione aziendale del Titolare, con indicazione di ciascun Trattamento effettuato all'interno di tale area.

Ogni scheda dovrà indicare, nel minimo, la categoria di interessato, il momento di raccolta del dato, le condizioni di liceità del Trattamento, le finalità del Trattamento, l'indicazione delle persone autorizzate al Trattamento, l'elencazione delle misure di sicurezza utilizzate per ciascun Trattamento e la valutazione del rischio.

11. Registro delle Attività di trattamento.

Ai sensi dell'articolo 30 del GDPR, FLASH LINE MAINTENANCE S.R.L., adotta un Registro delle Attività di Trattamento.

In conformità all'impostazione data dal presente MOTDP, il Registro delle Attività di Trattamenti di ciascuna società si compone della somma

delle Schede di Analisi Trattamenti effettuati presso ciascun Titolare, di cui al punto precedente. Il Titolare è responsabile della conservazione del Registro delle Attività di trattamento

12. Valutazione dei rischi e d'impatto nel trattamento dei dati

Ogni scheda di analisi dei trattamenti effettuati dovrà includere una valutazione dei rischi potenziali in caso di violazione dei dati personali. La valutazione dei rischi e di impatto per ogni trattamento è riportata all'interno della scheda di analisi dei trattamenti. Allegato 004.

13. Misure di sicurezza informatica

Riconoscendo l'importanza che la pianificazione ed implementazione di misure di sicurezza informatica assume per il rispetto dei principi di "privacy by design" e "by default" FLASH LINE MAINTENANCE S.R.L. nella figura del suo Titolare del Trattamento, ha adottato le seguenti policy e misure di sicurezza informatica:

- Archiviazione elettronica dei dati su PC client presenti nella sede centrale del Titolare del Trattamento
- Corretta gestione degli accessi ai documenti informatici a cura del personale
- Corretta gestione dei back up dei dati gestiti a livello informatico
- Adeguati sistemi di Firewall ed Antivirus al fine di scongiurare codici malefici

Al fine di tutelare i dati e le informazioni, il Titolare del trattamento ha adottato una specifica "Privacy Policy" nella quale sono descritte e dettagliate le specifiche misure di sicurezza e tutela.

14. Procedura di gestione delle richieste degli Interessati

Il Titolare del Trattamento rappresenta l'interfaccia unica per la raccolta delle richieste formulate dai vari interessati.

La casella di posta dedicata < privacy@f-lm.it> verrà indicata in tutte le informative emesse dal Titolare, sarà lo strumento per comunicare la volontà degli interessati di esercitare i diritti agli stessi garantiti dal GDPR.

Alla casella di posta potranno accedere il Referente Privacy/D.P.O ed il Titolare

Il Titolare o Referente Privacy/D.P.O. ha la responsabilità di esaminare le richieste ricevute, coinvolgere i Responsabili coinvolti dalla richiesta, dare riscontro all'interessato quanto alla presa in carico della richiesta, e provvedere a richiedere le azioni necessarie all'evasione della richiesta e da ultimo dare riscontro all'interessato quanto alle azioni intraprese.

15. Procedura di notifica in caso di violazione dei dati.

Chiunque all'interno di FLASH LINE MAINTENANCE S.R.L. abbia motivo di ritenere che vi sia stata una violazione dei Dati Personali trattati, ha l'obbligo di informare immediatamente il Titolare del trattamento, il Referente Privacy/D.P.O. e, ove presente, il Responsabile del Trattamento; specifica formazione sul punto verrà erogata a favore di tutti gli autorizzati al trattamento.

Ricevuta la segnalazione il Titolare del trattamento, il Referente Privacy/D.P.O. e, ove presente, il Responsabile del Trattamento, dovranno provvedere alla notifica all'autorità di controllo competente attraverso la compilazione dell'allegato 7, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento dell'accertamento.

La notifica all'Autorità di Controllo dovrà contenere:

a) La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) La comunicazione del nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire le informazioni contestualmente alla notifica dovrà essere formulata riserva di successiva integrazione.

Il Titolare del Trattamento mantiene un registro delle violazioni occorse come esplicitato al modulo 005.

16. DMMS – Documento delle Misure Minime Sicurezza

Il documento denominato DDMS – Documento Descrittivo Misure Sicurezza, in ottemperanza alle prescrizioni del D. L.gs. n. 196/2003 così come modificato dal D.lgs 101/2018 ("Codice della Privacy") e del Regolamento Europeo 679/2016, individua le azioni e le misure per il trattamento e la gestione dei dati in condizione di sicurezza, nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema di gestione descritto nel presente documento deve ritenersi idoneo in quanto intende garantire la disponibilità, l'integrità, e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi, la certificazione delle fonti di provenienza dei dati e le istruzioni per le persone autorizzate ad effettuare i relativi trattamenti, in relazione alle

diverse finalità dei trattamenti stessi.

Tale DDMS è stato inoltre progettato e concepito specificatamente per FLASH LINE MAINTENANCE S.R.L.

Una sorta di CODICE DI CONDOTTA specificatamente studiato ed elaborato ai sensi dell'art. 40 del regolamento Europeo 679:2016.

17. Allegati

000	Lettera di Impegno del Titolare del Trattamento
001	DDMS Documento Descrittivo Misure Sicurezza Anagrafica
002	Aziendale
003	Identificazione Titolare del trattamento
004	Scheda Trattamento e registro dei trattamenti
005	Registro delle Violazioni
006	Violazione Dati – Data Breach
007	Anagrafica sistemi Informatici
008	Elenco USER – PW
009	Elenco Responsabili del Trattamento
010	Elenco Incaricati interni / esterni
011A	Nomina del responsabile del trattamento interno Nomina del
011B	responsabile del trattamento esterno Informativa e Consenso
012	dipendenti
013C	Informativa e consenso Privacy Fornitori/Clienti – Azienda
014	Nomina DPO
014 bis	Attestazione DPO
015	Certificato QS_DPO_
016	Policy Posta elettronica aziendale
017	(IT POLICY ove presente)
018	Impegno di Riservatezza
019	/
020	Piano di Miglioramento
021	Elenco interventi formativi
022	Nomina Soggetto designato

FLASH LINE MAINTENANCE S.R.L.
VIA PASSO BUOLE 97 BC
00054 FIUMICINO RM
P.IVA 14546711004

D.D.M.S

Documento Descrittivo delle Misure di Sicurezza e di gestione e trattamento dei dati trattati

D.Lgs. 196/2003 così come modificato dal D.Lgs 101/2018

Regolamento Europeo 679/2016

Anno 2022

NOME AZIENDA	INDIRIZZO – Sede Centrale	PARTITA IVA
FLASH LINE MAINTENANCE S.R.L.	VIA PASSO BUOLE 97 BC - 00054 FIUMICINO	14546711004

Indice generale

1. SCOPO E FINALITA' DEL DOCUMENTO

Il presente documento denominato DDMS – Documento Descrittivo Misure Sicurezza, in ottemperanza alle prescrizioni del D. L.gs. n. 196/2003 così come modificato del D.Lgs 101/2018 ("Codice della Privacy") e del Regolamento Europeo 679/2016, individua le azioni e le misure per il trattamento e la gestione dei dati in condizione di sicurezza,nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema di gestione descritto nel presente documento deve ritenersi idoneo in quanto intende garantire la **disponibilità**, l'**integrità**, e l'**autenticità**, nonché la **riservatezza** dell'informazione e dei servizi per il trattamento, attraverso l'*attribuzione* di *specifici incarichi*, la *certificazione delle fonti di provenienza dei dati* e le *istruzioni per le persone autorizzate ad effettuare i relativi trattamenti*, in relazione alle diverse finalità dei trattamenti stessi.

Tale DDMS è stato inoltre progettato e concepito specificatamente per le aziende del gruppo di FLASH LINE MAINTENANCE S.R.L.
Una sorta di CODICE DI CONDOTTA specificatamente studiato ed elaborato ai sensi dell'art. 40 del regolamento Europeo 679:2016 come più avanti ampiamente descritto.

2. REQUISITI SPECIFICI DEL REGOLALENTO EUROPEO 679:2016

2.1 Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003 così come modificato del D.Lgs 101/2018 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Nell'art. 6 infatti si cita che:
Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

CONSENSO

• **Per i dati "sensibili"** (si veda art. 9 regolamento 679_2016) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su **trattamenti automatizzati (compresa la profilazione** – art. 22). Per i dati sensibili, inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

• **Per tutti gli altri dati** Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito"

• Deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

• Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

INTERESSE VITALE DI UN TERZO

• Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46).

INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO

• Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare; si tratta di una delle principali espressioni del principio di **"responsabilizzazione"** [ACCOUNTABILITY] introdotto dal nuovo pacchetto protezione dati.

• L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

2.2 informativa

I CONTENUTI DELL'INFORMATIVA

• I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

• Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

• Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

TEMPI DELL'INFORMATIVA

• Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

• Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un

linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).

• L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

• Sono inoltre parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

• L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato – art. 13 del regolamento).
Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

2.3 Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

• Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

• Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire 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; si veda anche art. 15, paragrafo 3).

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

• Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)

• L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

• Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/" oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica). In questo senso, in via generale, possono continuare a essere applicate tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento

2.4 Diritto di accesso (art. 15)

• Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento da parte dell'interessato.

• 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 terzi.

2.5 Diritto di cancellazione (diritto all'oblio) (art.17)

• Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

• Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).

2.6 Diritto di limitazione del trattamento (art. 18)

• Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, 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).

2.7 Diritto alla portabilità dei dati (art. 20)

• Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

• 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 ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli).

• Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Al riguardo, si ricordano i numerosi provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice (si vedano, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3251012 e, con riguardo all'attività bancaria in generale, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247).

Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

2.8 Approccio basato sul rischio e misure di accountability di titolari e responsabili

• Il regolamento pone con forza l'accento sulla **"responsabilizzazione" (accountability nell'accezione inglese)** di titolari e responsabili – ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

• Il primo fra tali criteri è sintetizzato dall'espressione **inglese "data Protection by default and by design"** (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

NB: Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

• Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da **obblighi di tenuta di un registro dei trattamenti** da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

2.9 Registro dei trattamenti

• Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

2.10 Misure di sicurezza

• Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

2.11 Responsabile della protezione dei dati

• Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/ responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano art. 38 e 39) in termini che Gruppo "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287).

3. DEFINIZIONI (Articolo 4 Regolamento 679/2016)

1)«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;

2)«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;

3)«LIMITAZIONE DI TRATTAMENTO»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4)«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;

5)«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;

6)«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;

7) «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;

8) «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;

9) «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 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT 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;

10) «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;

11) «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;

12) «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;

13) «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;

14) «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;

15) «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;

16) «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;
17) «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;

18) «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;

19) «GRUPPO IMPRENDITORIALE»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «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;

21) «AUTORITÀ DI CONTROLLO»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT

22) «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 sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «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;

24) «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;

25) «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 (1);

26) «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

4. I PASSI NECESSARI PER FLASH LINE MAINTENANCE S.R.L.

Nel seguito vengono indicati i passi necessari che FLASH LINE MAINTENANCE S.R.L. dovrà adottare per adempiere ai requisiti del nuovo Regolamento Europeo 679:2016 in modo efficace e senza eccessi di burocrazia e/o appesantimenti del sistema.
L'approccio utilizzato è quello del "CODICE DI CONDOTTA" esplicitato nell'art. 40 del Regolamento attraverso il quale è necessario dimostrare:

a) Il trattamento corretto e trasparente dei dati
b) I legittimi interessi perseguiti da Responsabile del Trattamento in contesti specifici
c) La raccolta dei dati personali
d) La pseudonimizzazione dei dati personali
e) L'informazione fornita al pubblico ed agli interessati
f) L'esercizio dei diritti agli interessati
g) L'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari delle responsabilità genitoriali sul minore
h) Le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'art. 32
i) La notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato
j) Il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali
k) Le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli art. 77 e 79.

I punti che saranno pertanto sviluppati sono i seguenti:

1. ANAGRAFICA AZIENDALE
2. IDENTIFICAZIONE DEL TITOLARE / CONTITOLARI DEL TRATTAMENTO
3. PRIVACY BY DESIGN – MAPPATURA DEI DATI
4. FINALITA' DEI DATI E TRATTAMENTI
5. REGISTRO DEI TRATTAMENTI E ANALISI RISCHI
6. DPIA – Data Protection Impact Assessment per RISCHIO ALTO
7. CONTROMISURE PER RISCHIO ALTO
8. ANAGRAFICA SISTEMI INFORMATICI, CRITERI DI ACCESSO E PROTEZIONE
9. SISTEMA DI AUTENTICAZIONE ACCESSI INFORMATICI E CREDENZIALI

10. IDENTIFICAZIONE E NOMINA RESPONSABILI
11. IDENTIFICAZIONE NOMINA INCARICATI
12. INFORMATIVE E LETTERE DI CONSENSO
13. INFORMATIVA IMPEGNO DI RISERVATEZZA
14. PROCEDURE SPECIFICHE PER TIPOLOGIE DI TRATTAMENTO PARTICOLARI
15. PROCEDURA PER EVENTO "DATA BREACHES"
16. POLICY PER POSTA ELETTRONICA
17. PROCEDURA SPECIFICA PER VIDEOSORVEGLIANZA (se applicabile)
18. IMPEGNI DI RISERVATEZZA
19. FORMAZIONE ED INFORMAZIONE

5. STRUTTURA DOCUMENTALE e OPERATIVA

Al fine di adempiere ai requisiti previsti dal Codice della Privacy ed a quanto previsto dal Regolamento 679:2016 ed in un'ottica di Privacy By Design ed Accountability il TITOLARE del TRATTAMENTO ha provveduto a progettare e implementare la seguente struttura documentale ed operativa, la cui attuazione viene esplicitata all'interno del MODELLO ORGANIZZATIVO – PRIVACY POLICY ed i relativi allegati in esso richiamati.

6. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA DEI DATI E LORO TRATTAMENTO

Al legale rappresentante, ovvero Titolare del Trattamento, Contitolare o eventualmente DPO nominato, è affidato il compito di aggiornare le misure di sicurezza relative la gestione e trattamento dei dati, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Nel caso di FLASH LINE MAINTENANCE S.R.L. il D.P.O/R.P.D è stato nominato con atto formale mediante Mod. 014 ed individua la persona di ……come DPO, del quale si allega evidenza formativa di certificazione della competenza ai sensi della NORMA 11697:2017 (allegato 015)

7. PIANO DI MIGLIORAMENTO – NO DATA BREACHES

L'impianto organizzativo e gestionale ed i sistemi di cui si è dotata l'organizzazione appaiono indicati nei documenti allegati, al fine di garantire le opportune misure di sicurezza relative il trattamento di dati da essa svolti.
In particolare, l'Allegato 8 esplicita, nel Piano di Miglioramento, le azioni che l'azienda si impegna a rendere operative al fine del miglioramento del sistema stesso.
Per miglioramento non si intendono le difformità e/o inadempiente al Regolamento che invece devono essere gestite con la procedura DATA BREACHES.
Eventuali variazioni o modifiche a quanto qui rappresentato OBBLIGA il titolare del trattamento all'aggiornamento del presente documento.

8. ELENCO DOCUMENTI ALLEGATI

I documenti allegati ed indicati nel MODELLO ORGANIZZATIVO- PRIVACY POLICY sono parte integrante degli adempimenti in materia di Privacy e dovranno essere compilati correttamente, custoditi e gestiti in conformità a quanto previsto dal presente DMMS e resi disponibili alle autorità di controllo.

9. DICHIARAZIONI D'IMPEGNO E FIRMA

Questo documento viene custodito presso la sede operativa dell'azienda, per essere esibito in caso di controlli.

Il Legale rappresentante – Titolare del Trattamento
DANIELE BALANI

Luogo e data:
ROMA 01-01-2022

MODELLO INFORMATIVA PRIVACY

Informativa ai sensi e per gli effetti di cui all'art. 13 Decreto legislativo 30 giugno 2003 n. 196 così come modificato dal D.Lgs 101/2018 (Codice in materia di protezione dei dati personali) e Regolamento 679/2016

Ai sensi dell'articolo 13 del D.Lgs. n° 196/2003 così come modificato dal D.Lgs 101/2018 ed artt. 13/14 del Regolamento Europeo 679/2016 recante il Codice in materia di protezione dei dati personali, la scrivente FLASH LINE MAINTENANCE S.R.L. con sede legale in VIA PASSO BUOLE 97 BC 00054 FIUMICINO in qualità di titolare del Trattamento (*nella persona DANIELE BALANI*) informa che i dati personali acquisiti in riferimento ai rapporti instaurati, formeranno oggetto di trattamento nel rispetto della normativa sopra richiamata e tale trattamento sarà improntato ai principi di *correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.*

a) *Finalità dei trattamenti cui sono destinati i dati*

I dati raccolti sono finalizzati all'espletamento dei seguenti trattamenti:

1. Finalità amministrative contabili dell'Azienda
2. Assolvimento di obblighi contrattuali, e quanto previsto dalla normativa vigente in materia di lavori, forniture e servizi aeroportuali
3. Esecuzione di contratti con Voi stipulati e dei connessi impegni, adempimento degli obblighi di Legge connessi al rapporto contrattuale, gestione organizzativa del contratto, collaborazioni professionali esterne contrattualizzate, per l'adempimento degli obblighi di Legge; tutela dei diritti contrattuali, analisi statistiche interne.

In occasione di tali trattamenti è possibile venire a conoscenza di dati che il Regolamento Europeo 679/2016 definisce sensibili (a titolo esemplificativo: **dati giudiziari, religione, orientamenti politici, situazioni familiari, etc.)**

b) *Modalità del trattamento*

Il trattamento sarà effettuato con sistemi manuali ed automatizzati atti a memorizzare, gestire e trasmettere i dati stessi, con logiche strettamente correlate alle finalità stesse, sulla base dei dati in nostro possesso e con l'impegno da parte Vostra di comunicarci tempestivamente eventuali correzioni, integrazioni e/o aggiornamenti. I dati verranno inseriti nelle pertinenti banche dati alle quali potranno accedere gli addetti incaricati al trattamento dei dati personali, che potranno effettuare operazioni di consultazione, utilizzo ed elaborazione, sempre nel rispetto delle disposizioni di Legge a garantire, tra l'altro, la riservatezza e la sicurezza dei dati, nonché l'esattezza, la conservazione, e la pertinenza rispetto alle finalità dichiarate.

Nell'ambito dei trattamenti descritti è necessaria la conoscenza e la memorizzazione di informazioni relative a dati anagrafici, codice fiscale, partita IVA, dati contabili.

L'eventuale non comunicazione, o comunque errata, di una delle informazioni indicate ha come conseguenza l'impossibilità del titolare di garantire la congruità del trattamento stesso ai patti contrattuali per cui esso sia eseguito;

c) *Natura di conferimento dei dati*

Il conferimento dei dati ed il relativo trattamento sono obbligatori in relazione alle finalità relative agli adempimenti di natura contrattuale e legale ed in relazione alle finalità che si riferiscono all'espletamento di tutte le attività della scrivente necessarie e funzionali all'esecuzione di obblighi contrattuali e legali. Il conferimento dei dati ed il relativo trattamento sono da ritenersi facoltativo nelle altre situazioni.

d) *Conseguenze di un eventuale rifiuto di rispondere*

Il Vs. eventuale rifiuto a prestare il consenso al trattamento dei dati per le finalità suddette, potrà determinare l'impossibilità della scrivente a dar corso ai rapporti contrattuali medesimi ed agli obblighi di legge.

e) *Ambito comunicazione e diffusione dei dati*

in relazione alle finalità indicate non è prevista la diffusione dei Vs. dati all'esterno, ma potranno essere comunicati ai seguenti soggetti o alle categorie di soggetti sottoindicati:

* Autorità Giudiziarie,

* Amministrazione Finanziaria, enti previdenziali ed assistenziali

* Autorità di Pubblica Sicurezza ed aeroportuale

* Banche ed Istituti di credito nell'ambito della gestione finanziaria dell'impresa

* Organismi associativi e consortili propri del settore

* Società che forniscono reti informatiche e telematiche

* Società di elaborazione dati contabili e redazioni adempimenti fiscali

* Società di servizi postali

* Società, enti, consorzi o altre organizzazioni avanti finalità di assicurazione, bancaria e simili nell'ambito delle attività svolte istituzionalmente dall'Agenzia delle entrate

* Società o enti di recupero del credito per le azioni relative

* Legali ed altri consulenti tecnici

I Sopracitati soggetti agiranno come autonomi titolari del trattamento.

I dati personali potranno essere trasferiti per le finalità dichiarate verso i Paesi dell'Unione Europea, alle categorie di soggetti sopra indicati se il trasferimento è necessario per l'esecuzione di obblighi derivanti da contratti di cui è parte l'interessato.

f) Titolare del trattamento dei dati personali

Il Titolare del trattamento è: FLASH LINE MAINTENANCE S.R.L.

I dati forniti saranno trattati da personale incaricato nominato e saranno conservati per tutta la durata del periodo contrattuale in essere. Oltre tale periodo valgono le disposizioni di legge specifiche per settore.

g) Diritti di cui all'art. 7 del D.Lgs 196/2003 così come modificato dal D.Lgs 101/2018

In ogni momento potrà esercitare i Suoi diritti nei confronti del Titolare del Trattamento, ai sensi dell'art. 7 del D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018, che per Sua comodità riproduciamo integralmente, nei limiti delle condizioni previste degli art. 8,9,10.

Decreto Legislativo 30 giugno 2003 n. 196 così come modificato dal D.Lgs. 101/2018 - Codice in materia di Protezione dei dati personali – Art. 7 Diritto di Accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno dei dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma leggibile.
2. L'interessato ha diritto di ottenere indicazione:
    a) Dell'origine dei dati personali;
    b) Delle finalità e delle modalità del trattamento;
    c) Della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
    d) Degli estremi identificativi del Titolare, dei Responsabili e del rappresentante designato ai sensi dell'art. 5 comma 2;
    e) Dei soggetti e delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
    a) L'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di Legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati trattati o successivamente trattati;

c) L'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) Per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) Al trattamento di dati personali che lo riguardano ai fine di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Tale diritto può essere esercitato rivolgendo un'istanza al titolare dei dati.

Titolare del Trattamento

DANIELE BALANI

_____

FLASH LINE MAINTENANCE S.R.L.
VIA PASSO BUOLE 97 BC
00054 FIUMICINO (RM)
P.IVA 14546711004

Modello Organizzativo Privacy (*Policy Privacy*)

Sommario

1. OBIETTIVI E DEFINIZIONI

IL TITOLARE DEL TRATTAMENTO DEI DATI (di seguito anche denominata "ente") intende dotarsi di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale

Obiettivo del presente documento e di quelli ad esso collegati è definire il **Modello Organizzativo Privacy (*Policy Privacy*)**, ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'ente, ai sensi del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (*GDPR – General Data Protection Regulamentation*), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente *policy*. In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali.

Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Regolamento: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- Normativa: D.Lgs. 2003/196 (come modificato dal D.Lgs. 2018/101) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy.
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Affiliate: società controllate o collegate al Titolare del trattamento dei dati stabilite nel territorio dello Stato italiano o in un luogo comunque soggetto alla sovranità dello Stato italiano;
- 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 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;
- 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;
- 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;
- Titolare del trattamento: la persona fisica preposta alla sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza se nominato da quest'ultimo, dal DPO;
- Titolare del trattamento: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati (o *designati)*;
- Autorizzato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (anche soggetti *designati*);
- 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 del trattamento o del responsabile del trattamento;
- 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;
- 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 inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);

2. AMBITO DI APPLICAZIONE

La **politica della privacy (*policy*)** che discende dal presente Modello Organizzativo Privacy si applica all'azienda nella sua interezza, a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

La sua attuazione è obbligatoria per tutto il personale e deve essere inserita come parte integrante nella regolamentazione di qualsiasi accordo con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nel campo del ***Sistema di Gestione della Privacy (SGP)***.

L'ente consente la comunicazione e la diffusione delle informazioni di tipo procedurale e organizzativo verso l'esterno esclusivamente per il corretto svolgimento delle attività aziendali che avvengono nel rispetto delle regole e delle norme vigenti.

L'ente si impegna a garantire e dimostrare che il trattamento dei dati personali avviene in maniera conforme a quanto previsto dalla normativa e, secondo i seguenti principi di liceità, questi sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui l'ente è Titolare, anche per tutti quei trattamenti di cui l'ente è nominato Responsabile del trattamento da altri Titolari del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.

Poiché analoghe garanzie di protezione e l'adozione di adeguate misure di sicurezza sono richieste ai soggetti terzi ai quali l'ente affida l'incarico di Responsabile del trattamento, la *policy* in oggetto è resa disponibile presso tali Responsabili del trattamento.

3. SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali l'ente assicura l'integrità e la

protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie e preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può infatti comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione della clientela, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo l'ente ha istituito e mantiene aggiornato un registro delle attività di trattamento.

L'ente identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi generali, di seguito enunciati:

- Esiste un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno di essi è individuato un responsabile;
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;
- Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente sottoposte a revisione (come previsto dal Regolamento Informatico);
- Sono definite delle procedure per l'utilizzo sicuro dei beni (luoghi, mezzi di trasporto, strumenti) e delle informazioni aziendali;
- È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;
- È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;

- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

4. RISERVATEZZA DELLE INFORMAZIONI

L'ente si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività in conformità alle procedure interne previste, coerenti con il presente Modello Organizzativo Privacy.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del codice civile.

L'ente si impegna a garantire adeguati livelli minimi di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

5. ATTUAZIONE DELLA *POLICY*

L'osservanza e l'attuazione della politica della privacy (*policy*) che discende dal presente Modello Organizzativo Privacy sono responsabilità di:

- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Privacy (SGP). Il personale è infatti responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda e che devono garantire il rispetto dei requisiti contenuti nella politica della privacy (*policy*);
- il titolare del trattamento quale responsabile del Sistema di Gestione della Privacy (SGP). Questi deve:
    - condurre l'analisi dei rischi con le opportune metodologie e adottare le misure per la gestione del rischio;

- stabilire le norme di comportamento necessarie alla conduzione sicura delle attività aziendali;
- verificare le violazioni alla sicurezza, adottare le contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
- organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la qualità, la sicurezza e la sicurezza delle informazioni;
- verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP).

Il personale dell'azienda che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno, potrà essere perseguito nelle opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.

6. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

La direzione aziendale verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP), in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

Il Titolare del trattamento, quale responsabile del Sistema di Gestione della Privacy (SGP), ha il compito di condurre operativamente la revisione di questa politica.

La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate.

Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy (SGP).

7. INFORMAZIONE E FORMAZIONE

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa[1], viene raggiunto dall'ente anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.

[1] Art. 29 Regolamento – "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento**"** Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
Art. 2 quaterdecies Codice Privacy – "Attribuzione di funzioni e compiti a soggetti designati" Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine dell'ente. Per gli stessi fini di conoscenza eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo creare un ecosistema favorevole nell'ambiente di lavoro e formare con particolare cura i soggetti che per il ruolo ricoperto risultano inseriti nel Sistema di Gestione della Privacy (SGP), l'ente:

- adotta un piano formativo con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali, destinato a tutto il personale della società;
- prevede l'erogazione di moduli specifici all'interno dei corsi di formazione per il ruolo ricoperto, sia in quelli organizzati all'immissione in servizio che al momento del cambio di mansione qualora sia di livello superiore o per ambito applicativo diverso;
- prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;
- conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione dei soggetti autorizzati al trattamento e, ove ritenuto necessario, delle altre figure chiave nel Sistema di Gestione della Privacy (SGP), riguarda in particolare:

- gli aspetti generali della disciplina di protezione dei dati personali;
- le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;
- le conseguenze derivanti dalla violazione dei dati personali (*Data Breach*);
- le procedure da seguire in caso di violazione dei dati personali;
- le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;
- gli aspetti specifici della disciplina di protezione dei dati personali nel settore di azione dell'ente;
- l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

La formazione deve essere:

- adeguata al proprio sistema di trattamento dei dati personali;

---

specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

- efficace nella trasmissione delle informazioni in materia di protezione dei dati personali;
- efficiente nel fornire strumenti per l'esecuzione delle procedure previste dal Sistema di Gestione della Privacy (SGP);
- documentabile, in quanto la formazione è parte integrante della *policy* dell'ente e l'articolazione e gli esiti di tale attività devono essere sempre disponibili.

8. IMPEGNO DEGLI ORGANI DI GOVERNO

La direzione dell'ente sostiene attivamente le attività inerenti la gestione della privacy, o protezione dei dati personali, tramite indirizzi precisi, impegno evidente, incarichi espliciti e riconoscimento delle responsabilità specifiche relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite un'adeguata struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi siano coerenti con la realtà della struttura a cui si riferiscono;
- stabilire i ruoli e relative responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione della Privacy (SGP);
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione della Privacy (SGP);
- controllare che il Sistema di Gestione della Privacy (SGP) sia integrato in tutti i processi aziendali e che le conseguenti procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

L'ente riconosce la propria responsabilità che discende dalla normativa vigente e si impegna a proteggere i dati personali che gli utenti affidano ad essa da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di tecnologie e procedure aziendali di protezione secondo le migliori pratiche (*best practices*) di volta in volta disponibili.

9. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITA'

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, l'ente garantisce sempre la precisa individuazione dei soggetti che ricoprono ruoli attivi

nel trattamento. Ciò avviene con l'allestimento e il mantenimento efficiente nel tempo di un sistema tracciabile delle nomine e delle relative mansioni.

In questo modo risulta di immediata comprensione la conseguente ripartizione delle responsabilità di ogni soggetto, parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati ogni volta ritenuto necessario.

Quanto descritto trova riscontro nell'organigramma privacy che viene aggiornato a cadenza periodica ritenuta più opportuna in relazione al settore di attività e all'articolazione della propria organizzazione oppure in occasione di qualsiasi variazione intervenuta.

In accordo con la normativa di riferimento e con la policy che discende dal presente Modello Organizzativo Privacy, costituiscono figure imprescindibili quelle di seguito descritte.

9.1 Titolare del Trattamento

Conformemente a quanto previsto dalla normativa l'ente è Titolare del trattamento e in tale ruolo si impegna a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

- diritto all'accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei

responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;

- diritto alla rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- diritto alla cancellazione, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- diritto all'opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, l'ente si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

9.2 Responsabile del Trattamento

Il Responsabile del trattamento dei dati è il soggetto, persona fisica o giuridica, nominato dal Titolare al fine di garantire nelle operazioni di trattamento l'attuazione delle misure di sicurezza previste dalla normativa e dal presente Modello Organizzativo Privacy.

Il soggetto preposto allo svolgimento della funzione viene individuato tra quelli in possesso dei necessari requisiti e con adeguate garanzie. Tra le sue funzioni sono comprese quelle di:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;

- nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- controllare le operazioni di trattamento svolte dai soggetti autorizzati sottoposti alla propria responsabilità e la conformità all'ambito di trattamento consentito;
- redigere e aggiornare la lista dei nominativi dei soggetti autorizzati sottoposti alla propria responsabilità e verificarne almeno annualmente l'ambito di trattamento consentito;
- proporre al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;
- distruggere i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento può modificare la propria struttura per conseguire i migliori risultati di protezione variando opportunamente l'articolazione del proprio Sistema di Gestione Privacy (SGP).

9.3 Soggetti autorizzati al trattamento

Il Titolare del trattamento (o il Responsabile del Trattamento) nomina, presso le Unità Organizzative in cui vengono svolti i trattamenti, i soggetti autorizzati al trattamento dei dati (o soggetto *designato*).

Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti l'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.

In particolare, i compiti a esso attribuiti sono così sintetizzati:

- segnalare al Titolare del trattamento, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- avvisare il Titolare del trattamento qualora, nello svolgimento di un'attività, dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di *privacy by design* e *privacy by default*;
- informare immediatamente il Titolare del trattamento qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al Titolare del trattamento eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

9.4 Amministratore di Sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (*system administrator*), ovvero una base dati (*database administrator*), ovvero reti e apparati di telecomunicazione di sicurezza (*network administrator*) è nominata persona autorizzata al trattamento dei dati personali con la qualifica specialistica di Amministratore di Sistema.

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

La nomina ad Amministratore di Sistema deve essere individuale, esplicitata in forma scritta, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

In generale, l'Amministratore di sistema ha le seguenti responsabilità:

- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il Titolare del trattamento fornire guida e supporto ai soggetti autorizzati in merito al trattamento dei dati personali;
- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, in merito a quanto previsto dal Regolamento Informatico del Sistema di Gestione della Privacy (SGP);

- individuare i soggetti a cui affidare l'incarico di manutentore del sistema stesso.

L'amministratore di Sistema che provvede alla designazione dei soggetti incaricati alla manutenzione deve preventivamente informare il Titolare del Trattamento e deve formalizzare per iscritto l'attribuzione dell'incarico eventualmente specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, allo stesso vengono concesse dal Titolare del trattamento le "Autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

L'elenco dei soggetti nominati Amministratori di Sistema è conservato adeguatamente.

10. MISURE DI SICUREZZA GENERALI

10.1 La gestione della sicurezza: ruoli e responsabilità

La responsabilità delle attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento sono in carico ai relativi ruoli inseriti nell'organico dell'ente. Tali sistemi possono essere sia logici che fisici e la responsabilità comprende la loro gestione diretta o tramite fornitori esterni.

In considerazione della complessità delle implicazioni relative alla sicurezza logica, è redatto il Regolamento Informatico del Sistema di Gestione della Privacy (SGP).

10.2 Misure per garantire la protezione dei dati

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Ad eccezione degli Amministratori di Sistema definiti e nominati secondo le disposizioni del Modello Organizzativo Privacy, nessun dipendente dell'ente è Amministratore di Sistema della propria macchina e tutti gli utenti che dispongono di una postazione informatica sono censiti.

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico dell'ente sono previste una serie di attività, in particolare al momento dell'assunzione o della dimissione delle risorse umane con la procedura di allestimento o dismissione dell'utenza personale. Sempre al fine di controllo si procede a verificare con cadenza semestrale che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

Tutti i dispositivi dell'ente concessi in dotazione ai dipendenti vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti dell'ente sono pertanto tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati e la conservazione dei documenti di lavoro.

10.3 Scrivania sgombra e schermo inattivo (*clean desk & clear screen Policy*)

La politica della ***scrivania sgombra*** (*Clean Desk Policy*) e dello **schermo inattivo** (*Clear Screen Policy*) è una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali (*Data Breach*) e responsabilizzare i soggetti che nelle attività lavorative si trovano a loro contatto.

Di seguito sono elencati i comportamenti virtuosi da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né possono essere lasciate per iscritto in posizione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;

- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento è soggetto alle azioni disciplinari previste, fino al licenziamento.

10.4 Livelli di sicurezza

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- applicazione del principio "*need to know*" o del minimo privilegio, secondo cui la definizione dei profili standard da assegnare agli utenti, con le autorizzazioni necessarie all'espletamento delle rispettive mansioni (definite per ruoli e competenze), avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica continua dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire un pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l'accesso da remoto, in particolare nei confronti di utenti appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, anche attraverso esercizi di *penetration test*, al fine di prevenire violazioni dei dati personali (*Data Breach*);
- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di sicurezza delle informazioni e di protezione dei dati personali;

- sono previsti periodici controlli al fine di verificare l'adeguatezza, l'affidabilità complessiva e la tutela del sistema informativo.