Modello Organizzativo Privacy
approvato dal Consiglio di Amministrazione il 19/12/2022

Sommario

PARTE GENERALE

CAPITOLO I – Il Regolamento UE 2016/679

1. Premessa

A far data dal 24 maggio 2016 è entrato in vigore il Regolamento UE n. 679 sulla protezione delle persone fisiche in relazione al trattamento dei dati personali e sulla libera circolazione dei dati medesimi. Occorre rilevare, in primis, che l'approccio proattivo peculiare della normativa, volto a proteggere i dati personali in via preventiva, rappresenta lo standard da sempre applicato da Formula Servizi Soc. Coop. (di seguito, per brevità, "Formula Servizi" o "Società" o anche "Organizzazione") nel costruire l'architettura del proprio sistema in materia di protezione dei dati personali, ivi incluso il profilo delle misure di sicurezza rilevanti ai fini della normativa privacy nazionale ed europea. Ciò posto, quindi, partendo da una struttura organizzativa già rispondente allo scopo di tutelare i dati personali e conforme ai dettati normativi del D.lgs. n. 196 del 30 Giugno 2003, nonché ai Provvedimenti dell'Autorità Garante per la protezione dei dati personali, la Società, ha implementato la propria struttura al fine di dare piena attuazione al Regolamento UE 2016/679 (di seguito, per brevità, anche "GDPR" o "Regolamento UE"), sia con riferimento agli obblighi di natura puramente formale, sia con riguardo agli adempimenti di natura tecnica, ivi incluso il profilo della sicurezza e tanto in veste di Titolare del trattamento, quanto in quella di Responsabile del trattamento.

Alla luce degli obblighi previsti dalla normativa privacy vigente, quindi, Formula Servizi Soc. Coop., nell'ambito della propria organizzazione, ha implementato la propria struttura al fine di garantire la conformità alla normativa anzidetta, adottando, tra l'altro, misure di sicurezza dei dati personali tali da garantire un livello adeguato di protezione dei dati medesimi.

In linea con la legislazione nazionale ed europea in materia di protezione dei dati personali e derivante, in particolar modo, dal Regolamento UE 2016/679 e dal D.lgs. n. 196/2003 coordinato ed aggiornato, da ultimo, con le modifiche apportate dalla L. n. 205/2021, nonché in conformità con gli le best practies e gli standard di settore in materia di sicurezza, nonché in adempimento ai provvedimenti, indicazioni e linee guida emanati dall'Autorità Garante per la Protezione dei dati personali e alle linee guida del Comitato europeo per la protezione dei dati (ex WP29), il presente Modello Organizzativo Privacy (di seguito, anche, "Mop") si propone la funzione di fornire alla struttura aziendale e ai soggetti coinvolti, a vario titolo, nell'adempimento degli obblighi posti dalla normativa a carico della Società, un valido strumento per il trattamento dei dati personali e per l'adozione delle misure di sicurezza e protezione dei dati personali. Il nuovo quadro normativo di riferimento, richiede, infatti, che il Titolare del trattamento proceda proattivamente e nel rispetto del principio di "accountability" alla previsione ed implementazione di misure organizzative e tecniche volte alla protezione dei dati personali e, comunque, nel rispetto dei principi generali e delle regole dettate dalla normativa privacy vigente. Il GDPR richiede, inoltre, che il Titolare del trattamento sia in grado di dimostrare che i trattamenti di dati personali siano conformi a quanto statuito dalla normativa; il presente Mop, pertanto, funge da "report" della conformità delle pratiche aziendali, finalizzate alla protezione dei dati personali, alla normativa di settore.

In accordo con la normativa summenzionata, la protezione dei dati personali può essere definita come la salvaguardia della Riservatezza (intesa come la garanzia che le informazioni siano accessibili ai soli soggetti autorizzati), dell'Integrità (intesa come l'accuratezza e completezza delle informazioni e del loro trattamento)

e della Disponibilità (intesa come la garanzia che i soggetti autorizzati abbiano agevole accesso alle informazioni quando richiesto o necessario) dei dati personali stessi.
I requisiti di sicurezza dei dati personali sono soddisfatti In virtù dell'implementazione di misure di sicurezza di varia natura quali, ad esempio, l'adozione di specifiche politiche e/o procedure, la precisa definizione di strutture organizzative ed individuazione delle funzioni assegnate al personale aziendale o l'adozione di tool o meccanismi tecnici. In altri termini, al fine di garantire il rispetto della normativa privacy vigente, la Società provvede al compimento delle seguenti attività:
-predisporre ed elaborare le proprie politiche di sicurezza dei dati personali in conformità ai principi sanciti dalla normativa nazionale ed europea;
-organizzazione il personale aziendale in modalità tali da limitare il trattamento dei dati personali a quanto effettivamente necessario e funzionale allo svolgimento delle funzioni assegnate, nonché formare, mediante appositi corsi, il personale anzidetto;
-inventariare le risorse e i trattamenti;
-regolamentare i rapporti con altri eventuali soggetti eventualmente coinvolti nel trattamento di dati personali, quali Responsabili del trattamento, Subresponsabili del trattamento o Contitolari;
-adottare misure di sicurezza, ivi incluse quelle tecniche (fisiche e logiche) e verificarne, periodicamente l'efficacia e la conformità alla normativa.
L'adozione dei principi generali e di buone pratiche nell'ambito della protezione dei dati personali, ivi incluso il profilo della sicurezza IT, nel quadro di conformità della normativa e dell'attuale organizzazione della società, permette di:

- Disporre di un valido strumento per adempiere agli obblighi di sicurezza e protezione dei dati personali previsti dalla normativa, nell'ottica di un costante miglioramento delle procedure della Società e della sua stessa struttura;
- Affrontare le problematiche di sicurezza attraverso un approccio coerente con la normativa;
- Accrescere la consapevolezza e diffondere la cultura della sicurezza dei dati personali nel contesto aziendale.

2. Quadro normativo di riferimento ex Regolamento UE 2016/679

Il GDPR definisce le "linee guida" da adottare in materia di Protezione delle Persone Fisiche con riguardo al Trattamento dei Dati nonché alla libera circolazione di tali dati. Si precisa, in prima battuta, che i "Dati" a cui si riferisce il Regolamento UE 2016/679 sono quelli che si riferiscono o che si possono in qualche modo ricondurre a Persone Fisiche e, dunque, non anche alle persone giuridiche (come, ad esempio, le aziende).
Con la sua introduzione, inoltre, il GDPR costituisce un prezioso strumento per armonizzazione le regole privacy dei vari Stati appartenenti all'Unione Europea e per sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software.
Ulteriore rivoluzione introdotta dal GDPR nel sistema di protezione dei dati personali è il "principio di accountability", ovvero il c.d. principio di responsabilizzazione. Tale principio, di fatto, attribuisce più discrezionalità ma, al tempo stesso, maggiore responsabilità al "Titolare del Trattamento" su tutto quello che concerne la protezione dati personali, con un inasprimento consistente delle sanzioni previste in caso di inadempienza. Infatti, il Titolare ed il

Responsabile del Trattamento, indipendentemente dalla circostanza che si tratti di soggetto pubblico o di soggetto privato, hanno il preciso dovere di dimostrare le ragioni che hanno determinato le scelte fatte in materia privacy. A tal fine, occorre dimostrare che:
– sono state implementate le misure di sicurezza adeguate ed efficaci a protezione dei dati e che tali misure sono costantemente riviste e aggiornate in considerazione delle attività in concreto svolte;
–i trattamenti sono conformi ai principi e alle disposizioni del regolamento europeo, compresa l'efficacia delle misure anzidette.
In tale ottica, l'adesione ai codici di condotta ex art.40 del GDPR o ad un meccanismo di certificazione ex art.42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi previsti dalla normativa privacy vigente a carico dei soggetti pubblici o privati che svolgano il trattamento di dati personali. Parallelamente, al fine di poter dimostrare la conformità alle disposizioni del regolamento, è l'obbligo di tenuta di registro delle attività di trattamento, anche in formato elettronico, con relativa descrizione delle misure di sicurezza applicate (ex. art. 30 del GDPR). In riferimento al profilo della sicurezza del trattamento, il GDPR, all'art. 32, prevede che il Titolare ed il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Il principio di accountability anzidetto consente di realizzare una concreta protezione della posizione giuridica delle persone fisiche, c.d. soggetti interessati, i cui dati personali costituiscono oggetto di trattamento.
A tali ultimi soggetti sono riconosciuti, infatti, una serie di specifici diritti privacy, previsti agli artt. 15 e ss del GDPR, ovvero il diritto di accesso ai dati personali, il diritto di rettifica dei dati personali, il diritto all'oblio, il diritto di limitazione del trattamento, il diritto alla portabilità dei dati dei dati personali, il diritto di opposizione al trattamento ed il diritto di non essere sottoposto ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.
Parallelamente alla maggiore attenzione nei confronti della posizione dei soggetti interessati, il GDPR ha previsto un rafforzamento dei poteri delle Autorità Garanti nazionali ed un inasprimento delle sanzioni amministrativo a carico di imprese e pubbliche amministrazioni: nel caso di violazioni dei principi e disposizioni del regolamento, le sanzioni, in casi particolari possono arrivare fino a 10 milioni di euro o per le imprese fino al 2%-4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

3. Ulteriori riferimenti normativi in materia di trattamento dei dati personali

Contestualmente al GDPR, ai fini del presente Mop trovano applicazione i riferimenti normativi individuati nel prosieguo. Resta intesto che la relativa elencazione ha carattere puramente esemplificativo e non esaustivo ed è comunque soggetta alle eventuali modifiche ed integrazioni normative, nonché all'assunzione, da parte dell'Autorità Garante per la Protezione dei Dati Personali e del Comitato europeo per la protezione dei dati, di nuovi ed ulteriori provvedimenti.

- D.Lgs. 104 del 27-06-2022 "Attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea";
- D.Lgs. n. 196/2003 adeguato al GDPR con il Decreto legislativo 10 agosto 2018, n. 101 e modificato, da ultimo, con le modifiche apportate dalla L. n. 205/2021;

- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 23 novembre 2006, in materia di trattamento dei dati personali dei lavoratori privati;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 1 marzo 2007, in materia di posta elettronica e internet;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 13 ottobre 2008, in materia di Raae e misure di sicurezza dei dati personali;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 8 aprile 2020, in materia di videosorveglianza;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27 novembre 2008, in materia di amministratori di sistema;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 4 luglio 2013, in materia di attività promozionale e contrasto allo spam;
- Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 12 novembre 2014, in materia di biometria;
- Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021;
- Legge n. 633 del 22 aprile 1941 (c.d. "Legge sul diritto d'autore");
- Linee guida del Comitato europeo per la protezione dei dati.

4. Definizioni

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.

DATO PERSONALE: Qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. soggetto interessato); si considera identificabile la persona fisica che può esser 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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

CATEGORIE PARTICOLARI DI DATI: Dati personali idonei a rilevare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

SOGGETTO INTERESSATO: Persona fisica a cui si riferiscono i dati personali oggetto di trattamento.

DATI GIUDIZIARI: Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza.

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

RESPONSABILE DEL TRATTAMENTO: Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

SUBRESPONSABILE DEL TRATTAMENTO: Organismo di cui un Responsabile del trattamento può avvalersi nel trattamento dei dati personali effettuato per conto di un Titolare del Trattamento. In capo al Sub-Responsabile del Trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto nazionale o dell'Unione, gli stessi obblighi assunti, in materia privacy, dal Responsabile del Trattamento con il Titolare del Trattamento.

AUTORIZZATO AL TRATTAMENTO: Chiunque, agendo sotto l'autorità del Titolare o del Responsabile del trattamento, acceda e, in generale, tratti i dati personali. Il relativo trattamento dovrà avvenire nel rispetto delle istruzioni impartite dal Titolare o Responsabile del trattamento

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI: Figura introdotta dal GDPR alla quale il Titolare o il Responsabile del trattamento affidano funzioni di controllo e supporto in relazione all'adempimento degli obblighi previsti dalla normativa privacy vigente. Tale figura ha, altresì, funzioni consultive, formative, informative relativamente all'applicazione del GDPR, anche coaudivando il Titolare o il Responsabile del trattamento nell'adozione delle misure di sicurezza e di ogni garanzie necessaria ai fini del trattamento dei dati personali.

REGISTRO DEL TRATTAMENTO: Documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.

DATA BREACH: Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

VALUTAZIONE DI IMPATTO: Onere posto direttamente a carico del titolare del trattamento, volto ad assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali. Si tratta di valutazione da svolgere prima di iniziare il trattamento circa le conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Tale valutazione dovrà esser eseguita ogni volta in cui un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

CAPITOLO II – Gli organismi nazionali ed europei in materia di protezione dei dati personali

1. Le autorità a sorveglianza della normativa in materia di trattamento dei dati personali

Nel prosieguo sono individuati i principali organismi nazionali ed europei rilevanti in materia di protezione dei dati personali e proposti a garantire il rispetto della normativa privacy vigente.
In particolar modo, ai fini del presente documento, sono illustrate le principali attività svolte dai seguenti organismi:

- Autorità Garante per la protezione dei dati;
- Garante europeo per la protezione dei dati;
- Comitato europeo per la protezione dei dati.

1.1 Autorità Garante per la protezione dei dati

Ogni Stato membro dell'Unione europea ha una propria Autorità di controllo che vigilia, a livello nazionale, sul rispetto della normativa privacy vigente.
Il Garante per la protezione dei dati è l'autorità di controllo italiana in ambito di protezione dei dati personali. Si tratta, in particolar modo, di un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (Legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196) ed i cui compiti sono attualmente definiti da quest'ultimo, oltre che dal GDPR.
In particolare, tale autorità si occupa principalmente di:
- verificare la conformità alla legge dei trattamenti e prescrivere ai titolari le misure da adottare;
- esaminare i reclami per eventuali violazioni del GDPR e delle norme nazionali in materia di protezione dei dati;
- limitare, sospendere o vietare i trattamenti in violazione delle norme;
- adottare le autorizzazioni generali;
- promuovere codici di deontologia e condotta (es. in materia di giornalismo);
- partecipare alle attività comunitarie e internazionali;
- irrogare sanzioni correttive.

Con il GDPR, il Garante per la Protezione dei dati personali interviene principalmente ex post, cioè la sua valutazione si colloca successivamente alle valutazioni del Titolare del trattamento, con abolizione delle notifiche preventive dei trattamenti e sostituzione con obblighi di tenuta di un registro dei trattamenti e da valutazioni di impatto autonome da parte del Titolare del trattamento.
Il Garante per la Protezione dei Dati Personali è contattabile ai seguenti riferimenti:

Email: protocollo@gpdp.it
PEC: protocollo@pec.gpdp.it
Telefono: +39 06.696771

1.2 Il Garante europeo per la protezione dei dati

Il Garante europeo per la protezione dei dati è l'autorità europea di sorveglianza indipendente, istituita nel 2004 e con sede a Bruxelles (Belgio), il cui obiettivo primario è garantire che le istituzioni e gli organi dell'Unione europea rispettino il diritto alla vita privata e alla protezione dei dati personali.
In particolare, tale autorità provvede a:

- controllare il trattamento dei dati personali da parte dell'amministrazione dell'UE allo scopo di assicurare il rispetto delle norme sulla privacy;
- fare da consulente per le istituzioni e gli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazione;
- gestire le denunce e conduce indagini;
- collaborare con le amministrazioni nazionali dei paesi dell'UE per assicurare la coerenza nell'ambito della protezione dei dati;
- controllare le nuove tecnologie che possono influire sulla protezione dei dati.

Il Garante è nominato per un mandato rinnovabile di 5 anni. Per svolgere le sue funzioni, l'autorità conta su due sezioni principali di cui una esamina il rispetto della protezione dei dati da parte delle istituzioni e degli organi dell'UE e l'altra fornisce consulenza ai legislatori dell'UE su aspetti concernenti la protezione dei dati attinenti alle politiche di diversi settori e a nuove proposte legislative.

1.3 Comitato europeo per la protezione dei dati

Con l'introduzione del GDPR nell'impianto normativo in materia di protezione dei dati personali, il Comitato europeo per la protezione dei dati ha sostituito il precedente "Gruppo di lavoro articolo 29" e consiste nel gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.
E' un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati (EDPS), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta.
Il Gruppo adotta le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo.
L'articolo 70 del GDPR prevede, appunto, vari compiti da affidare ai membri dei Garanti nazionali, che quindi si riuniscono allo scopo di:

- assicurare l'applicazione corretta del GDPR, fatti salvi i compiti delle autorità nazionali di controllo;
- fornire consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione;
- pubblicare linee guida, raccomandazioni e prassi al fine di promuovere l'applicazione coerente del regolamento e sulle materie previste;
- esaminare, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del regolamento;
- effettuare l'accreditamento di organismi di certificazione e il suo riesame periodico;

- fornire alla Commissione pareri per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale;
- promuovere la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale;
- promuovere programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;
- emettere pareri sui codici di condotta;
- tenere un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

Il suo compito principale è garantire il principio di congruità e coerenza, cioè assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia privacy.

CAPITOLO III – Il Modello Organizzativo Privacy di Formula Servizi Soc. Coop.

1. Il Modello Organizzativo Privacy adottato da Formula Servizi Soc. Coop.

Formula Servizi è nata il 24.10.1975 con il nome di Pulix Coop. Società Cooperativa a responsabilità limitata dall'accordo di nove soci fondatori con l'obiettivo di perseguire l'interesse generale delle comunità alla promozione umana e alla integrazione sociale dei cittadini attraverso lo svolgimento delle attività di pulizia. Negli anni la Società è cresciuta e dal 2001 la ragione sociale è divenuta Formula Servizi Soc. Coop. ed oggi offre sul mercato, tra gli altri, servizi di sanificazione e pulizie in ambito pubblico e privato, anche sanitario, servizi di facchinaggio e logistica, servizi di archiviazione cartacea e digitale, servizi di facility ed edilizia, portierato, call center, servizi culturali e servizi di restauro.

La Società è retta e disciplinata dai principi della mutualità senza fini di speculazione privata.

Il Modello Organizzativo Privacy adottato in Formula Servizi è stato condotto sulla base dell'analisi dei rischi in relazione alle fattispecie rilevanti ai fini della normativa privacy vigente, considerando tutti i processi operanti in Cooperativa.

2. Finalità del Modello Organizzativo Privacy

Attraverso l'adozione del Mop Formula Servizi si propone di perseguire le seguenti principali finalità:

- la conformità dei trattamenti alla normativa privacy vigente;
- l'efficacia delle migliori misure scelte e adottate nelle attività di trattamento;
- garantire la continuità nel tempo del percorso di conformità alla normativa privacy vigente, anche a fronte di eventuali variazioni dell'assetto dell'Organizzazione;
- rapportarsi con le autorità di controllo con un percorso di compliance ben strutturato e definito, che possa anche fornire alle autorità dei punti di riferimento nell'effettuazione dei controlli o nel percorso di verifica.
- rendere consapevoli tutti i destinatari del Mop, come nel prosieguo individuati, dell'esigenza di un puntuale rispetto del Mop stesso, alla cui violazione possono conseguire sanzioni in capo alla Società;
- informare in ordine alle gravose conseguenze che potrebbero derivare alla Società dalla violazione della normativa privacy vigente;
- consentire alla Società un costante controllo ed un'attenta vigilanza sulle attività, in modo da poter intervenire tempestivamente ove si manifestino profili di rischio in materia di trattamento dei dati personali ed eventualmente applicare le misure disciplinari previste dallo stesso Modello.

Più specificatamente, il presente Mop, pertanto, è redatto con lo scopo di garantire la conformità ai principi e alle prescrizioni in materia di protezione dei dati personali e di sicurezza previsti dalla normativa privacy vigente e di fornire al personale aziendale un supporto per il corretto adempimento degli obblighi della normativa anzidetta, che vengono in rilievo in fase di esecuzione delle mansioni lavorative che, tipicamente, comportano il trattamento di dati personali. A tal

fine, il presente documento si prefigge lo scopo di fungere da manuale guida a sostegno dell'esecuzione di operazioni di trattamento poste in essere dal personale nell'esecuzione delle proprie mansioni, nonché da sistema di organizzazione e raccolta della principale documentazione privacy in uso nel contesto aziendale.
Nell'ambito degli obblighi generali previsti dagli artt. 24 e 32 del GDPR, il presente Mop si propone di:
-assicurare l'adozione di misure di sicurezza idonee a garantire un livello adeguato di protezione dei dati personali trattati;
-rappresentare un valido strumento per il costante miglioramento delle misure di sicurezza adottate al fine di allinearle alle nuove conoscenze acquisite in virtù del progresso tecnico, nonché al fine di parametrarle, costantemente, alla natura dei dati personali e alle caratteristiche del trattamento, in modo tale da ridurre al minimo i rischi di distruzione, perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta dei dati medesimi.
La protezione e la sicurezza dei dati personali è realizzata mediante misure di sicurezza di natura fisica (e.g. protezione delle aree e dei locali dove sono ubicati gli archivi cartacei che contengono dati personali e gli strumenti elettronici impiegati nel trattamento di dati personali) e organizzative (procedure, norme e istruzioni per la corretta gestione delle attività, individuazione dei ruoli, compiti e responsabilità del personale in materia di sicurezza e protezione dei dati personali) adottate dal Titolare del trattamento, dai Responsabili esterni del trattamento, dagli amministratori di sistema e dai soggetti autorizzati al trattamento dei dati personali.
Con il presente Mop, pertanto, la Società intende descrivere il modello organizzativo adottato in ambito privacy, sia con riguardo all'ipotesi in cui operi in qualità di Titolare del trattamento, sia con riguardo all'ipotesi in cui operi come Responsabile o Sub-Responsabile del trattamento.
Con riferimento al primo profilo, il presente Mop analizza, in particolar modo, le modalità e i limiti del trattamento dei dati personali dei propri lavoratori che, a qualsiasi titolo, prestino la propria mansione a favore della Società, nonché le garanzie poste a tutela dei soggetti medesimi, con particolare attenzione agli obblighi di informazione, posti a carico della Società, in considerazione del rapporto di lavoro, nonché ai diritti esercitabili dai lavoratori in considerazione di suddetto trattamento.
Con riferimento al secondo profilo, invece, il presente documento mira a descrivere il modus operandi adottato, sotto il profilo privacy, dalla Società in fase di erogazione dei servizi offerti ai propri Clienti, pubblici o privati. Nell'individuazione delle regole applicate al trattamento dei dati personali riconducibili ai propri Clienti, la Società, in un'ottica di conformità alla normativa privacy vigente e al principio di accountability, tiene conto della tipologia e natura dei servizi, in concreto, erogati a favore dei Clienti anzidetti.
I principi e le istruzioni previsti nel presente Mop, nonché i documenti allegati, ancorché non materialmente, allo stesso, si applicano all'intera struttura societaria, compatibilmente con la tipologia e natura di trattamenti in concreto svolti dai singoli uffici o dei diversi settori coinvolti nelle attività svolte dalla Società.

3. Efficace attuazione del Modello Organizzativo Privacy

L'efficace attuazione del Mop richiede:

- la divulgazione e messa a disposizione del MOP a tutti i lavoratori e collaboratori della Società, nonché a tutti coloro che, in considerazione dei rapporti commerciali in essere con la Società, possano trattare i dati personali di cui la Società stessa sia Titolare, Responsabile o Subresponsabile ai sensi della normativa privacy;
- la verifica periodica della congruità del MOP rispetto alla normativa privacy vigente e l'eventuale modifica dello stesso alla luce di eventuali mutamenti della normativa anzidetta ovvero quando siano scoperte significative violazioni delle prescrizioni in esso previste ovvero quando intervengano mutamenti nella Società o nelle attività da essa perseguite;
- la predisposizione di una procedura di gestione delle violazioni di dati personali che abbia riguardo anche al profilo della valutazione della condotta del lavoratore e collaboratore della Società o del Partner di quest'ultima, la quale condotta abbia compromesso la posizione dei soggetti interessati alla luce della normativa privacy vigente.

4. La divulgazione del Modello Organizzativo Privacy

La Società si attiva per informare tutti i potenziali destinatari in ordine al contenuto dispositivo del Mop ed, in particolar modo, a garantire adeguata diffusione delle "parte generale" del presente documento ad ogni dipendente e collaboratore di Formula Servizi, nonché ai soggetti esterni che possano essere coinvolti nel trattamento di dati personali rilevanti per la Società, ovvero ai Partner commerciali che, in particolar modo, agiscano in veste di Responsabili o Subresponsabili del trattamento per conto di Formula Servizi.

Di conseguenza, ogni comportamento posto in essere da tali destinatari in contrasto con le linee di condotta indicate dal presente Mop e tale da comportare una potenziale violazione dei dati personali trattati ai sensi della normativa privacy, potrà assumere rilevanza ai fini disciplinari in relazione al personale della Società, comunque nel rispetto del CCNL applicabile, nonché potrà determinare la rivalutazione dei rapporti commerciali in essere rispetto ai Partner della Società.

4.1 Informazione e formazione del personale

Ai fini dell'efficacia del presente Mop, è obiettivo di Formula Servizi garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti del proprio personale. Tale obiettivo riguarda tutte le risorse della Società, sia quelle già presenti in Formula Servizi sia quelle da inserire.

In particolar modo, al fine di garantire la conoscenza della normativa privacy è prevista la pubblicazione del presente documento all'interno dell'area riservata del Portale aziendale dedicato al personale della Società.

Parallelamente Formula Servizi fornisce al proprio personale un'adeguata conoscenza in materia privacy mediante appositi corsi di formazione svolti dalla Società ed erogati in modalità e-learning. A tal fine la Società ha definito un programma di formazione per il personale.

L'attività di formazione potrebbe anche esser differenziata in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza:

4.2 Informazione ai Partner commerciali

Relativamente ai Partner commerciali, ovvero, ai fini del presente Mop, ai fornitori di servizi di Formula Servizi, ivi inclusi quelli che operino in qualità di subappaltatori in relazione ai Clienti della Società stessa, Formula Servizi garantisce un'adeguata informativa in merito all'esistenza del Modello Organizzativo Privacy, relativamente alla sua parte principale e dei principi in esso contenuti.

Il mancato rispetto da parte dei Partner commerciali dei principi in materia di protezione dei dati personali espressi nel presente documento, può comportare una rivalutazione, da parte della Società, della posizione del Partner.

5. Integrazione fra Modello Organizzativo Privacy e del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01

Il Consiglio di Amministrazione di Formula Servizi ha approvato, in data 17.12.2012, il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 (di seguito, per brevità anche "Mog") che individua le procedure operative sviluppate dalla Società per ridurre il rischio che apicali e sottoposti commettano reati a vantaggio o interesse di questa ultima**.**

Il Modello di Organizzazione, Gestione e Controllo discende dal D.Lgs. n. 231/2001 pertinente alla responsabilità degli Enti per gli illeciti amministrativi dipendenti da reato commessi da persone fisiche nell'interesse o a vantaggio degli enti stessi, scardinando quel granitico principio secondo il quale "*Societas delinquere non potest*".

Il Dlgs 231/2001 disciplina una particolare forma di responsabilità giuridica che ha natura sostanzialmente penale, poiché sorge in dipendenza di un fatto di reato, accertata all'interno di un processo penale.

I destinatari della normativa sono:

- le società e le associazioni fornite di personalità giuridica (tra cui le società di capitali e le società cooperative iscritte nel registro delle imprese);
- le associazioni, fondazioni ed altre istituzioni di carattere privato senza scopo di lucro;
- le società di capitali e cooperative e tutti gli enti privati sprovvisti di personalità giuridica (le associazioni non riconosciute).

Nella fattispecie, oltre alle sanzioni pecuniarie, esistono le sanzioni interdittive, come:

-l'interdizione dall'esercizio dell'attività;

-l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

-il divieto di contrattare con la pubblica amministrazione;

-la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito.

L'art. 6 del suddetto decreto contempla una forma di esonero di responsabilità qualora l'Ente dimostri di aver adottato ed efficacemente attuato un Mog idoneo a prevenire la realizzazione dei reati considerati, comprovando che la commissione del reato non è etiologicamente collegabile ad una propria "colpa organizzativa".

In fase di valutazione circa il Modello Organizzativo Privacy da elaborare ed adottare, la Società ha ritenuto di dare rilievo, nella Parte Speciale del presente documento nell'ambito del quale vengono evidenziate le principali attività e dunque anche i trattamenti svolti dalla diverse aree della Società, alle procedure che

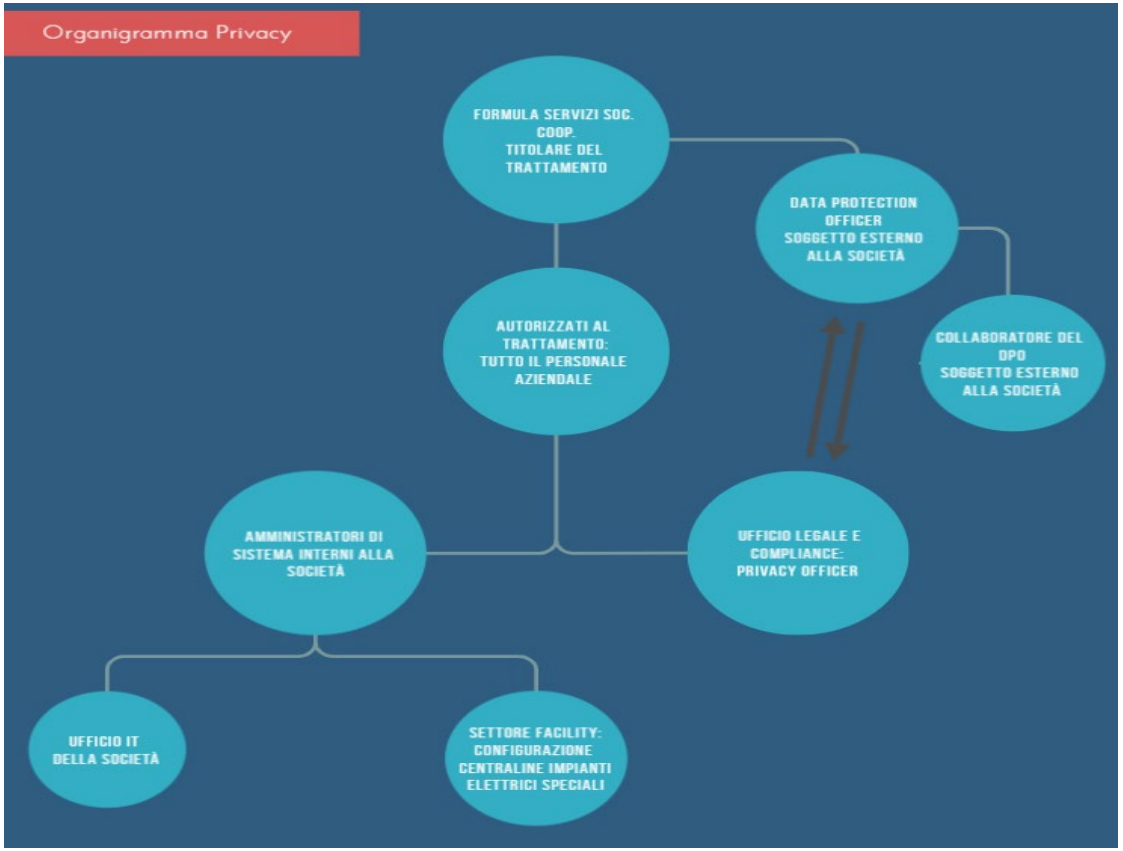
compongono il Modello Organizzativo ex D.Lgs 231/01, in un'ottica di integrazione di due diversi modelli, Mog e Mop, anche al fine di amplificare il "rating di legalità" evitando sanzioni pecuniarie e interdittive.
Ai fini di tale integrazione, pertanto, la Società, nella Parte Speciale del Mop, ha provveduto ad analizzare gli eventuali profili privacy emergenti nell'ambito delle procedure che compongono il Mog, in particolar modo evidenziando eventuali lacune, svolgendo valutazioni in merito alle possibili modifiche od integrazioni da appartare alle procedure stesse per garantire la piena conformità delle scelte aziendali alla normativa vigente in materia di trattamento dei dati personali.

CAPITOLO IV – La struttura privacy di Formula Servizi Soc. Coop.

1. Organigramma Privacy di Formula Servizi Soc. Coop.

Di seguito è riportato l'**Organigramma privacy** della Società.

Si precisa che, nell'ottica della Società, l'organigramma costituisce il primo e fondamentale requisito per adempiere al principio di *accountability*, in quanto consente l'individuazione degli attori principali nell'ambito del trattamento dei dati personali. Infatti, ai fini della responsabilizzazione del Titolare del trattamento, così come richiesta dal GDPR, è fondamentale individuare i ruoli privacy, sia al fine di distinguere i soggetti con funzioni operative privacy e quelli con poteri di controllo e supervisione, nonché al fine della definizione di eventuali responsabilità che vengano in rilevo nell'ambito del trattamento dei dati personali.



2. La funzione di Data Protection Officer

Il GDPR ha introdotto nell'ordinamento la nuova funzione del "Data Protection Officer" (di seguito, per brevità, "DPO"), ovvero del Responsabile della Protezione dei dati personali.

Tale funzione, che può essere interna od esterna all'organizzazione che tratta i dati personali e che potrà consistere in un organo monocratico o collegiale, è destinata ad esser coinvolta in tutte le questioni riguardanti la protezione dei dati personali e, ai fini della sua funzione, deve essere in possesso di specifici requisiti di competenza, esperienza, indipendenza e autonomia di risorse, assenza di conflitti di interesse. Principale compito del DPO è quello presidiare i profili privacy organizzativi attraverso un'opera di sorveglianza sulla corretta applicazione della normativa privacy vigente e delle policy interne in materia di protezione dei dati personali, sull'attribuzione delle responsabilità all'interno delle organizzazioni che trattano dati, nonché sul rispetto, da parte di queste ultime, degli obblighi di informazione, sensibilizzazione e formazione del personale, fornendo consulenza e rilasciando pareri. Inoltre, il DPO ha il compito di cooperare con l'Autorità Garante per la Protezione dei Dati Personali e costituisce un punto di riferimento e di contatto per i soggetti interessati che ad esso possono rivolgersi per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento europeo. L'identità ed i dati di contatto del DPO devono essere riportati, nell'ottica di trasparenza verso i soggetti interessati, nelle informative privacy da rendere prima dell'inizio del trattamento dei dati personali.

La Società ha provveduto a nominare il Data Protection Officer, contattabile all'indirizzo e-mail:

dpo@formulaservizi.it

La nomina del DPO è stata comunicata all'Autorità Garante per la Protezione dei Dati Personali che detiene un apposito registro dei nominativi di tutti i **DPO** presenti sul territorio italiano.

Il DPO svolge audit periodici al fine di tenersi aggiornato ed esprimere, se del caso, eventuali pareri in merito all'andamento delle attività in materia di trattamento dei dati personali da parte della Società. All'esito di tali audit, il DPO provvede a redigere apposito verbale, messo a disposizione della Società.

3. La funzione di Privacy Officer

Il Privacy Officer è una figura professionale con competenze giuridiche, informatiche e gestionali, la cui responsabilità principale è osservare, valutare e organizzare la gestione del trattamento di dati personali all'interno di un'organizzazione, affinché questi siano trattatati nel rispetto della normativa privacy vigente.

La funzione di Privacy Officer della Società è interna ed è collocata nell'ambito dell'Ufficio Legale e Compliance. Tale funzione è contattabile all'indirizzo e-mail:

privacy@formulaservizi.it

La funzione di Privacy Officer collabora costantemente con il Data Protection Officer della Società, adempiendo ai compiti di informazione nei confronti di quest'ultimo. In particolare, la funzione di Privacy Officer provvede ad informare il DPO dell'andamento delle attività privacy della Società nel corso degli audit da questo ultimo svolti, nonché a comunicargli, mediante apposite segnalazioni, gli eventi che potrebbero comportare una violazione dei dati personali trattati dalla

Società, nonché eventuali responsabilità di Formula Servizi ai sensi della normativa privacy vigente, nonché a richiedere pareri in merito a questioni rilevanti in materia di protezione dei dati personali.

4. Amministratori di sistema

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. L'Autorità Garante per la protezione dei dati personali, inoltre, considera tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Così come previsto dall'Autorità Garante anzidetta nelle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008, modificato in base al provvedimento del 25 giugno 2009, Formula Servizi, ai fini dell'attribuzione delle funzioni di amministratore di sistema al proprio personale, provvede a svolgere una preventiva valutazione in merito ai requisiti dell´esperienza, della capacità e dell´affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
Gli amministratori di sistema di Formula Servizi sono designati mediante apposita nomina individuale che include, peraltro, l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
Nell'ambito della Società, le categorie di personale a cui sono attribuite le funzioni di amministratore di sistema sono riconducibili a tre classi:

- Personale aziendale appartenente all'Ufficio IT;
- Personale aziendale eventualmente preposto alla gestione e alla manutenzione di sistemi di videosorveglianza o di sue componenti;
- Persone aziendale appartenente al settore facility ed a cui sia stata affidata l'attività di configurazione centraline impianti elettrici speciali.

Gli estremi identificativi del personale di Formula Servizi che opera in qualità di amministratore di sistema, con l´elenco delle relative funzioni, sono resi disponibili all'interno dell'area riservata del Portale aziendale dedicato al personale della Società e possono comunque esser sempre richiesti scrivendo all'indirizzo e-mail:

privacy@formulaservizi.it

La Società verifica, con cadenza annuale, l'attività svolta dal proprio personale che opera in qualità di amministratore di sistema al fine di verifica il rispetto della normativa privacy vigente, ivi incluso il profilo della sicurezza.
Ancorché non materialmente allegato al presente Mop, l'"Atto di nomina ad amministratore di sistema interno" costituisce parte integrante e sostanziale di tale documento.

La Società si avvale di un sistema di registrazione dei log che consente di tracciare e registrare le attività di accesso ai sistemi da parte degli stessi amministratori di sistema. Le registrazioni (access log) corrispondono alle caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste e comprendono i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate.

5. Autorizzati al trattamento dei dati personali

Sono autorizzati al trattamento dei dati personali tutti i dipendenti e collaboratori di Formula Servizi che operano sotto la diretta autorità di quest'ultima. I dipendenti e collaboratori della Società, infatti, nell'esecuzione delle specifiche mansioni lavorative affidategli trattano o possono trattare dati personali di cui Formula Servizi è Titolare, Responsabile ovvero Subresponsabile del trattamento. A tal fine, Formula Servizi provvede, con apposito documento fornito in fase di assunzione, ad autorizzare il proprio personale all'esecuzione delle operazioni di trattamento anzidette, fornendo le necessarie istruzioni per l'esecuzione di corrette operazioni di trattamento dei dati personali.
Ancorché non materialmente allegato al presente Mop, l'"Autorizzazione al trattamento di dati personali" costituisce parte integrante e sostanziale di tale documento.

6. L'Organismo di Vigilanza: il chiarimento dell'Autorità Garante per la protezione dei dati personali circa posizione privacy dell'OdV

Con una nota prot. 17347 del 12 maggio 2020, il Garante per la protezione dei dati personali ha precisato che l'Organismo di Vigilanza (di seguito, per brevità, anche "OdV"), previsto dall'articolo 6 del D.Lgs. 231/2008, non è un Titolare del trattamento e neppure un Responsabile esterno ex art. 28 del GDPR.
Come precisato dall'Autorità, l'Organismo di Vigilanza, indipendentemente dalla circostanza che i membri che lo compongano siano interni o esterni, è da considerare "parte dell'ente". Pertanto, in considerazione del trattamento dei dati personali implicato dall'esercizio dei compiti e delle funzioni affidate all'OdV, lo stesso ente, Titolare del trattamento, deve designare i singoli membri dell'OdV quali soggetti autorizzati. Tali soggetti, di conseguenza, in relazione al trattamento dei dati degli interessati, dovranno attenersi alle istruzioni impartite dal titolare affinché il trattamento avvenga in conformità ai principi stabiliti dall'articolo 5 del GDPR.
Secondo l'Autorità, infatti, se è vero che l'Organismo di Vigilanza esercita i compiti che gli sono attribuiti dalla legge, attraverso "autonomi poteri di iniziativa e controllo", è anche vero tale Organismo opera nell'ambito dell'organizzazione dell'ente, Titolare del trattamento, il quale determina il perimetro e le modalità di esercizio di tali compiti.
L'Odv, pertanto, non può essere considerato autonomo Titolare del trattamento, considerato che i compiti di iniziativa e controllo propri dell'OdV non sono determinati dall'Organismo stesso, bensì dalla legge che ne indica i compiti e dall'organo dirigente che nel modello di organizzazione e gestione definisce gli aspetti relativi al funzionamento compresa l'attribuzione delle risorse, i mezzi e le misure di sicurezza.
In adempimento all'impostazione dell'Autorità Garante per la protezione dei dati personali, pertanto, Formula Servizi ha provveduto a nominare i componenti dell'Organismo di Vigilanza della Società quali soggetti autorizzati al trattamento.

CAPITOLO V – Le sanzioni ex Regolamento UE 2016/679

1. Il sistema sanzionatorio previsto dal GDPR

Il GDPR disciplina, agli articoli 83 e 84, le sanzioni da applicare in caso di violazione della normativa in materia di trattamento dei dati personali. In particolare, il GDPR disciplini esclusivamente le sanzioni amministrative: la normativa in oggetto prevede, infatti, all'articolo 84, che ciascuno Stato disciplini autonomamente le sanzioni penali. Nel caso dell'Italia si è scelto di mantenere in vigore le sanzioni penali già previste dal già citato Codice della privacy.
Ai sensi del GDPR le sanzioni privacy possano arrivare fino a 20 milioni di euro, e colpiscano fino al 2% o al 4% del fatturato annuo delle imprese non conformi alla normativa. Il testo del regolamento prevede, poi, che le sanzioni applicate vengano comminate in base ai criteri di effettività, proporzionalità e dissuasività. In Italia, per eseguire i controlli sugli adempimenti obbligatori, oltre a Funzionari dell'Autorità Garante della protezione dei dati personali, è stata incaricata la Guardia di Finanza.
Pertanto, le possibili conseguenze per le imprese che agiscano in violazione del GDPR comprendono:

- sanzioni amministrative;
- sanzioni penali;
- condanna al risarcimento del danno;
- divieto temporaneo di trattamento dei dati personali (fino a che non venga ripristinata una condizione di conformità alla normativa).

1.1 Le sanzioni amministrative pecuniarie introdotte dal GDPR

Come anticipato, il GDPR disciplina nel dettaglio soltanto le sanzioni amministrative, che hanno quindi natura pecuniaria. In particolare, l'articolo 83 del GDPR prevede sanzioni *fino a*:

- 10 milioni di euro o 2% del fatturato mondiale annuo dell'anno precedente per le imprese nei casi in cui, per esempio, i dati personali dei soggetti interessati vengano trattati in maniera illecita, non venga nominato il DPO, non venga comunicato un Data Breach all'Autorità garante;
- 20 milioni di euro o 4% del fatturato per le imprese nei casi più gravi, come ad esempio l'inosservanza dei diritti degli interessati o il trasferimento illecito di dati personali ad altri Paesi.

Il GDPR non prevede un valore *minimo* per la sanzione, che pertanto dovrà essere commisurata dall'Autorità Garante sulla base dei criteri di effettività, proporzionalità e dissuasività.

Sempre l'articolo 83, poi, prevede numerosi criteri che devono orientare il Garante nella quantificazione della sanzione. In particolar modo di segnala:

- il comma 2, lett. d), dove si afferma che si deve tenere debito conto del "grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32";
- il comma 2, lett. j), che parla dell'"adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42.

1.2 Le sanzioni penali

Le violazioni delle disposizioni in materia di privacy non comportano soltanto sanzioni amministrative, ma possono dar luogo anche a responsabilità di tipo penale. L'articolo 84 del GDPR prevede che siano gli Stati membri a disciplinare le sanzioni previste in caso di violazioni che non sono già punite con sanzioni amministrative. In Italia, come già precisato, per le sanzioni penali a tutela della privacy si è scelto di mantenere in vigore quanto stabilito dal Codice della Privacy del 2003, ed in particolare dagli articoli 167 e successivi, così come riformati, che disciplina cinque differenti violazioni, punite con sanzioni penali che arrivano fino a sei anni di reclusione:

- *Trattamento illecito dei dati*. Si tratta di un reato comune, nel senso che può essere commesso da chiunque; perché si integri la fattispecie è necessario che ricorra il dolo specifico, cioè la volontà di trattare illecitamente i dati personali al fine di trarne un guadagno economico oppure di danneggiare la vittima. Quando per lo stesso fatto è stata applicata a norma del GDPR una sanzione amministrativa dal Garante e questa sia stata riscossa, la pena viene diminuita;
- *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*;
- *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*;
- *Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*;
- *Inosservanza dei provvedimenti del Garante*. Si precisa che non ogni violazione dei provvedimenti costituisce reato, ma solamente la trasgressione di precisi provvedimenti adottati dall'Autorità Garante, ovvero, fra gli altri, dei provvedimenti di limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento, dei provvedimenti con i quali l'Autorità stabilisce le misure di garanzia funzionali ad autorizzare, ma in senso restrittivo, il delicato campo del trattamento dei dati genetici, biometrici e relativi alla salute. Per tutti gli altri casi, l'inosservanza dei provvedimenti del Garante è punita con una sanzione amministrativa.

2. I controlli e le ispezioni

Il GDPR ha rivoluzionato il sistema sanzionatorio in materia di privacy: mentre in passato si interveniva solo a posteriori, ora la violazione si riscontra già nel momento in cui l'impresa non metta in atto le misure preventive utili a tutelare i cittadini.

Anche con riferimento alla fase dei controlli, delegati alla Guardia di Finanza, è fondamentale il concetto di accountability, vale a dire "responsabilizzazione" dei Titolari del trattamento dei dati personali: durante le ispezioni, gli Enti avranno l'onere di mostrare cosa è stato fatto e se qualcosa non è stato fatto, dovranno dimostrare le ragioni del mancato adempimento.
Tipicamente, le attività di ispezione svolte dalla Guardia di Finanza si concentrano principalmente su:

- nomina del DPO, il responsabile della protezione dati;
- controlli sulle misure previste in caso di Data Breach;
- controlli sul registro dei trattamenti.

Muovendo proprio dal concetto di responsabilizzazione, il senso dell'ispezione è proprio quello di verificare quali valutazioni e scelte sono state fatte dagli Enti; in questo senso, il presente Mop costituisce un valido strumento per palesare le attività privacy realizzate dalla Società e dimostrare le logiche poste alla base delle attività stesse.
Si precisa, inoltre, che la Società ha provveduto all'elaborazione di un'apposita "Procedura per le visite ispettive da parte dell'Autorità di controllo". Ancorché non materialmente allegata al Mop, l'anzidetta procedura costituisce parte integrante e sostanziale del presente documento.

CAPITOLO VI – Linee guida in materia di trattamento dei dati personali

1. Le linee guida di Formula Servizi per il compimento delle operazioni di trattamento dei dati personali

Nel compimento delle operazioni di trattamento dei dati personali, Formula Servizi procede nel rispetto dei principi fissati all'articolo 5 del GDPR, ovvero:

- *liceità, correttezza e trasparenza* del trattamento, nei confronti dell'interessato;
- *limitazione della finalità del trattamento*, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- *minimizzazione dei dati*: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- *esattezza e aggiornamento dei dati*, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- *limitazione della conservazione*: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- *integrità e riservatezza*: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Così come previsto dalla normativa privacy applicabile, la Società tratta i dati personali solo in considerazione dell'esistenza di un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del GDRP e possono consistere nei fondamenti di seguito individuati:

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

Per quanto riguarda le "categorie particolari di dati personali" (e.g. dati sanitari)**,** il loro trattamento è vietato, in prima battuta, a meno che il Titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del GDPR, che qui ricordiamo:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:
    - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

- per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

1.1 L'obbligo di informazione nei confronti dei soggetti interessati: l'informativa privacy

Prima di iniziare un trattamento di dati personali, la Società provvede fornire ai soggetti interessati la relativa "informativa privacy", al fine di chiarire tutti gli aspetti rilevanti relativi al trattamento stesso, nonché al fine di porre tali soggetti nelle condizioni di esercitare i diritti privacy. In particolar modo, i contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del GDPR e, in parte, sono più ampi rispetto al Codice. Il Titolare del trattamento deve sempre specificare i dati di contatto del 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. Se i dati non sono raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, inoltre, 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.

Il GDPR prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il Titolare del trattamento 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.

L'informativa viene fornita ai soggetti interessa prima di effettuare il trattamento, quindi prima della raccolta dei dati. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa, ex art. 14 del GDPR, 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).

1.2 L'analisi dei rischi e la valutazione di impatto privacy

Nell'ottica del principio di accountability, l'art. 24 del GDPR richiede che ciascun titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, avendo condotto una preventiva analisi dei rischi che impattano sui diritti e le libertà delle persone, metta in atto misure tecniche e organizzative adeguate a garantire e dimostrare. Dunque, prima dello svolgimento delle attività di trattamento è necessario effettuare la relativa analisi dei rischi. Nella Parte Speciale del presente Mop sono individuati i parametri applicati dalla Società a cui quest'ultima ricorre per lo svolgimento di una preventiva analisi dei rischi che consenta di calcolare il livello di rischio intrinseco dell'attività svolta, valutare i controlli già implementati, calcolare quindi il livello di rischio residuo per l'organizzazione e pianificare il suo piano di trattamento secondo le modalità ritenute più opportune. Di contro, l'art. 35 del GDPR prevede la valutazione di impatto privacy che va svolta quando a seguito del procedimento di analisi dei rischi, potrebbe risultare, per una o più attività di trattamento, un livello di rischio elevato. In particolare, la valutazione di impatto deve essere svolta quando:
-il trattamento comporta una valutazione sistematica e globale di aspetti relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

-si debba svolgere il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1, del GDPR o di dati relativi a condanne penali e a reati di cui all'art. 10;

-il trattamento comporta la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Ai fini dello svolgimento della valutazione di impatto, la Società si avvale del software messo a disposizione dall'Autorità Garante Francese e scaricabile dal sito www.cnil.fr https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

1.3 La tenuta del Registro del trattamento

Formula Servizi provvede alla tenuta di un registro delle operazioni di trattamento dei dati personali, collocato, in particolar modo, nella Parte Speciale del presente Mop.
In particolar modo, l'art. 30 del GDPR prevedere che tutti i Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti - ma solo se non effettuano trattamenti a rischio – debbano tenere un registro delle operazioni di trattamento, i cui contenuti sono indicati all'articolo anzidetto.
Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un Ente, indispensabile per ogni valutazione e analisi del rischio. I contenuti del registro sono fissati nell'articolo 30. Tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.
Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

1.4 Gli adempimenti privacy per il trattamento dei dati personali dei lavoratori a seguito del "Decreto Trasparenza"

Il 13 agosto 2022 è entrato in vigore il D.Lgs. 104 del 27-06-2022 "Attuazione della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea", che attribuisce ai datori di lavoro nuovi obblighi informativi al momento della stipula di un contratto o di una lettera di assunzione .

In particolare, il datore di lavoro è obbligato ad "*informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori […]*" precisando altresì che le informazioni devono essere comunicate "*in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico*".

Pertanto, con l'entrata in vigore di detta disposizione, la Società, in quanto datore di lavoro, con riferimento ai citati sistemi decisionali e di monitoraggio automatizzati, provvede ad informare il proprio personale:

a) sugli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi anzidetti;
b) sugli scopi e le finalità dei sistemi anzidetti;
c) sulla logica ed il funzionamento dei sistemi anzidetti;
d) sulle categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi anzidetti, inclusi meccanismi di valutazione delle prestazioni;
e) sulle misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
f) sul livello di accuratezza, robustezza e cybersicurezza dei sistemi anzidetti e le metriche utilizzate per misurare tali parametri, nonchè gli impatti potenzialmente discriminatori delle metriche stesse.

A tal fine, la Società ha provveduto ad integrare l'informativa privacy rilasciata al proprio personale in fase di assunzione, tenendo anche conto degli esiti dell'analisi dei rischi e della valutazione di impatto svolta in relazione ai trattamenti dei dati personali del personale di Formula Servizi che comportino l'uso di sistemi decisionali e di monitoraggio sistematico.

1.5 La gestione delle potenziali violazioni di dati personali

Formula Servizi ha provveduto alla predisposizione di un'apposita procedura di gestione e segnalazione delle violazioni dei dati personali che la coinvolgano, sia nella sua posizione di Titolare del trattamento che nella posizione di Responsabile del trattamento.

Ai sensi del GDPR, infatti, tutti i Titolari del trattamento dovranno notificare all'Autorità Garante per la protezione dei dati personali le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se ritengono probabile che da tale violazione derivino rischi per i diritti e le

libertà degli interessati (considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per i soggetti interessati che spetta al Titolare del trattamento.
Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche i soggetti interessati, sempre "senza ingiustificato ritardo".
I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del GDPR.
La Società, inoltre, documenta, mediante redazione di appositi verbali, tutte le potenziali violazioni di dati personali subite, anche se non notificate all'Autorità Garante e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.
La procedura di gestione e segnalazione delle violazioni di dati personali adottata dalla Società è allegata al presente documento (ALLEGATO A "Gestione e Segnalazione Evento Data Breach") e ne costituisce parte integrante e sostanziale per presente documento.
In particolare, l'anzidetta procedura si applica, nel rispetto delle Norme UNI EN ISO 9001:2015, ai seguenti casi:
1) quando la Società operi come *Titolare del trattamento,* determinando le finalità e i mezzi del trattamento di dati personali;
2) quando la Società operi quale *Responsabile del trattamento* nominata dai propri Clienti in relazione ad uno specifico contratto di fornitura dei servizi e quindi, quando tratti dati personali per conto dei propri Clienti Titolari del trattamento.
La procedura si applica al personale dipendente e ai collaboratori della Società, autorizzati al trattamento dei dati personali di cui la Società è Titolare o Responsabile, che vengano a conoscenza di una violazione dei dati personali. In conformità a quanto statuito dalla procedura in oggetto, la gestione, da parte della Società, della potenziale violazione dei dati personali implica la realizzazione delle seguenti fasi:

- Fase 1: Identificazione e indagine preliminare
- Fase 2: Contenimento e recovery
- Fase 3: Eventuale notifica all'Autorità Garante
- Fase 4: Documentazione della violazione

Si precisa, infine, che una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. A titolo esemplificativo, il data breach può essere dovuto a:

- Perdita accidentale
- Furto
- Infedeltà aziendale
- Accesso abusivo.

1.6 La formazione al personale aziendale

Formula Servizi eroga appositi corsi di formazione in materia privacy a favore del proprio personale. Tali corsi sono svolti in modalità e-learning e sono finalizzati a garantire la conoscenza della normativa privacy vigente al fine di consentire il corretto compimento delle operazioni di trattamento sui dati personali. A tal fine la Società ha redatto apposito cronoprogramma che, ancorché non materialmente allegato al Mop, costituisce parte integrante e sostanziale del presente documento.

Infatti, Il GDPR ha rafforzato ulteriormente l'importanza della formazione privacy all'interno degli Enti, rendendola una misura di sicurezza obbligatoria per tutti i dipendenti e collaboratori e non solo per figure specializzate come il Data Protection Officer o il Privacy Officer. La mancata formazione privacy è considerata una violazione di legge ed è soggetta al pagamento di una sanzione amministrativa sino a 20.000.000 di euro o al 4% del fatturato di gruppo.
La Società non considera la formazione privacy come un mero adempimento burocratico, bensì un'opportunità per rendere consapevoli i propri operatori dei rischi connessi al trattamento dei dati e delle misure di sicurezza. Tutto questo consente non solo di evitare rischi di sanzioni amministrative, ma anche di migliorare la reputazione della Società, nonché l'organizzazione dei processi interni e l'erogazione dei servizi.
Si precisa, altresì, che nel prosieguo sono definite le linee guida che il personale aziendale è tenuto a rispettare in fase di trattamento dei dati personali per conto della Società.

1.7 La gestione dei rapporti con i Fornitori di servizi

Ai fini della gestione dei rapporti con i Fornitori che eroghino servizi direttamente a favore di Formula Servizi ovvero a favore dei Clienti di quest'ultima, la Società, relativamente ai casi in cui l'erogazione degli anzidetti servizi comporti il compimento di operazioni di trattamento sui dati personali di cui Formula Servizi è Titolare o Responsabile del trattamento, la Società provvede a nominare i fornitori stessi Responsabili o Subresponsabile del trattamento. A tale scopo la Società provvede a richiedere ai fornitori la sottoscrizione del Contratto di nomina a Responsabile o Subresponsabile del trattamento elaborato ai sensi del GDPR e che prescrive le regole da applicare al trattamento dei dati personali svolti per conto di Formula Servizi, anche con riguardo al profilo della sicurezza. I relativi contratti, ancorché non materialmente allegato al Mop, costituiscono parte integrante e sostanziale del presente documento.
Si precisa, altresì, che nel prosieguo sono definite le linee guida che i fornitori di servizi sono tenuti a rispettare in fase di trattamento dei dati personali per conto della Società.

1.8 L'esercizio dei diritti privacy da parte dei soggetti interessati

Formula Servizi garantisce ai soggetti interessati l'esercizio dei propri diritti privacy di cui agli artt. 15 e ss del GDPR. A tal fine, la Società ha predisposto l'apposita "Procedura di riscontro delle istanze dei diritti degli interessati" la quale, ancorché non materialmente allegata al Mop, costituisce parte integrante e sostanziale del presente documento.
Con riferimento ai soggetti interessati, infatti, il GDPR stabilisce che i Titolari del trattamento devono rispettare le modalità previste per l'esercizio di tutti i diritti da parte dei soggetti interessati, stabilite, in via generale, negli artt. 11 e 12 della normativa anzidetta.
In particolare, 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 del trattamento a dover dare riscontro in caso di esercizio dei diritti, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio di tali diritti.

Il Titolare del trattamento ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee. Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), pari a 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.

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.

Spetta, inoltre, al Titolare del trattamento 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 - ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso. 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.

2. Linee guida in materia privacy per il personale di Formula Servizi Soc. Coop.

In fase di trattamento dei dati personali svolto in considerazione dell'esecuzione delle mansioni lavorative, la Società richiede ai propri lavoratori il rispetto di specifiche regole di condotta di cui le principali sono riportate nel prosieguo.

In linea generale, il personale deve effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal citato Regolamento, in relazione a cui è informato mediante la formazione privacy e tutte le policy della Società.

Il personale si impegna a rispetto l'obbligo di riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti ad essa assegnati, anche successivamente alla cessazione del rapporto di lavoro o collaborazione;

In particolare, il personale è tenuto a:

-Trattare i soli dati la cui conoscenza sia necessaria e sufficiente per l'esecuzione delle proprie mansioni;

-Conservare gli strumenti aziendali e/o supporti cartacei contenenti dati personali in modo da evitare che detti strumenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

-Con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate senza mantenerne copia; quando tali atti e i documenti contengano dati particolari o dati giudiziari, il personale deve controllare e custodire i medesimi atti e documenti con particolare diligenza e cura fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione;

-Non effettuare copie di Dati Personali su Device Mobili, a meno di espressa autorizzazione di Formula Servizi. In ogni caso, tali supporti non devono mai essere lasciati incustoditi e al termine del trattamento devono essere riconsegnati a Formula Servizi. I Device Mobili, se non utilizzati, devono essere consegnati a Formula Servizi affinché li distrugga, li resetti o li renda inutilizzabili nei modi indicati da Formula Servizi.

-Curare, in caso di utilizzo autorizzato di Device Mobili, che i dati personali in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori (devono essere utilizzati soltanto supporti vergini o vuoti);

-Dare immediata comunicazione a Formula Servizi nel caso si constati o si sospetti un incidente di sicurezza (ossia le violazioni di sicurezza che comportano 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), scrivendo a databreach@formulaservizi.it;
-Mantenere la massima riservatezza sui dati personali dei quali venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
-Svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, da Formula Servizi e, comunque, in modo lecito e secondo correttezza;
-Fornire a Formula Servizi, a semplice richiesta e secondo le modalità indicate da questa, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
-Prestare la più ampia e completa collaborazione a Formula Servizi al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
-Custodire con dovuta diligenza ogni strumento di accesso ai locali aziendali di Formula Servizi o di terzi ai quali è stato autorizzato ad accedere;
-Non scattare foto o fare video ai locali ove svolge la propria mansione, salvo in presenza di diversa autorizzazione da parte di Formula Servizi;
-Non scattare foto o fare video a persone o documenti presenti nei locali ove svolge la propria mansione, salvo in presenza di diversa autorizzazione da parte di Formula Servizi;
-Non trascrivere informazioni personali relative agli utilizzatori dei locali ove svolge la propria mansione, salvo in presenza di diversa autorizzazione da parte di Formula Servizi e, comunque, non sottrarre documento od oggetti;
-Non portare a terzi informazioni personali relative agli utilizzatori dei locali ove svolge la propria mansione;
-Non accedere al contenuto dei cassetti, armadi o cestini dei rifiuti, salvo non sia necessario in considerazione della propria mansione
-Non pubblicare sui social e comunque diffondere in rete o mettere a disposizione di soggetti terzi, immagini o video che riprendono e/o ritraggono contesti lavorativi, soggetti terzi e il marchio e logo aziendale.
- Relativamente alle banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su strumenti aziendali altrui o su strumenti personali e non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
-Modificare il proprio codice di accesso in base a quanto stabilito dalle policy di sicurezza di Formula Servizi;
-Non comunicare o rendere conoscibile a terzi il proprio codice di accesso.

3. Linee guida in materia privacy per i fornitori di servizi di Formula Servizi Soc. Coop.

In fase di erogazione dei servizi che comportino il trattamento dei dati personali, la Società richiede al relativo Fornitore, che operi nella qualità di Responsabile o Subresponsabile del trattamento, il rispetto delle seguenti prescrizioni.

a) Il Fornitore è legittimato a trattare i dati personali esclusivamente nei limiti di quanto necessario ai fini dell'erogazione dei servizi, nonché a compiere le relative operazioni di trattamento soltanto su istruzione documentata della Società. In particolare, il Fornitore si astiene dall'utilizzare i dati personali per finalità proprie e comunque diverse dall'esecuzione dei servizi a favore della Società;

b) Il Fornitore tratta i dati personali nel rispetto dei principi generali previsti ai sensi dell'art. 5 del Regolamento UE e dunque in modo lecito, corretto e secondo trasparenza, provvedendo, ove necessario, alla correzione ed aggiornamento dei dati personali. Inoltre, le operazioni di trattamento devono esser compiute riducendo al minimo l'utilizzo dei dati personali in conformità al principio di minimizzazione dei dati personali di cui al Regolamento UE.
I dati personali sono trattati per finalità determinate, esplicite e legittime in conformità a quanto stabilito dal Titolare. I dati personali devono essere pertinenti, completi e non eccedenti rispetto alle finalità individuate dal Titolare. La conservazione dei dati personali va limitata al periodo di tempo necessario al perseguimento delle finalità per cui i dati stessi sono stati raccolti e trattati;

c) Il Fornitore garantisce che il proprio personale aziendale, in concreto preposto al compimento delle operazioni di trattamento sui dati personali, sia stato vincolato, mediante sottoscrizione di appositi accordi, alla segretezza e alla riservatezza con riferimento ad ogni informazione, ivi inclusi i dati personali, di cui possa venire a conoscenza nell'esecuzione della prestazione lavorativa. Inoltre, il Fornitore è tenuto ad istruire, anche attraverso corsi di formazione periodici, il personale anzidetto con riguardo alla materia della protezione dei dati personali al fine di garantire che le operazioni di trattamento avvengano nel rispetto di quanto definito nella normativa applicabile in materia di trattamento dei dati personali.
Resta inteso che il Fornitore provvede a vigilare sull'operato del proprio personale aziendale e verifica, periodicamente, il rispetto dell'obbligo alla segretezza e alla riservatezza, nonché la conformità delle operazioni svolte alle istruzioni ricevute dalla Società e alla normativa suindicata.

d) Il Fornitore è tenuto a conformarsi al Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27 novembre 2008 nell'ipotesi in cui, in considerazione della particolare natura del servizio erogato a favore della Società, il proprio personale aziendale operi in qualità di amministratore di sistema. A tal fine, il Fornitore provvede a identificare e designare per iscritto gli amministratori di sistema, previa valutazione in ordine alle caratteristiche di capacità, affidabilità ed esperienza dei soggetti designati e conserva ed aggiorna il documento recante gli estremi identificativi degli amministratori di sistema.
Il Fornitore è tenuto a verificare, con cadenza almeno annualmente, che le attività svolte dagli amministratori di sistema rispondano alle misure organizzative, tecniche e di sicurezza predisposte a garanzia dei trattamenti dei dati personali.
E' onere del Fornitore garantire la tracciabilità e la registrazione dell'attività di accesso da parte degli amministratori di sistema quando, ai fini dell'erogazione dei servizi a favore della Società, venga utilizzato il sistema informativo del Fornitore stesso. Le relative registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni, inoltre, devono comprendere i riferimenti

allo "*username*" utilizzato, i riferimenti temporali e la descrizione dell'evento (*log in* e *log out*) che le ha generate e devono essere conservate per un periodo congruo, non inferiore a sei mesi;

e) Il Fornitore accede ai database che contengono i dati personali trattati esclusivamente ai fini dell'erogazione dei servizi e si astiene, altresì, dal creare database ulteriori, salvo il caso in cui tale attività sia necessaria per l'erogazione dei servizi stessi e fermo restando il rispetto dell'obbligo di comunicazione preventiva dell'attività medesima nei confronti del Fornitore
Inoltre il Fornitore, in assenza di specifica indicazione della Società, si astiene dal creare copie o duplicati dei dati personali e dall'asportare supporti informatici contenenti i dati personali trattati;

f) Il Fornitore è tenuto ad implementare, applicare e tenere costantemente aggiornate le misure tecniche ed organizzative richieste dalla normativa primaria e secondaria, tempo per tempo vigente, in materia di protezione dei dati personali ed applicabile ai servizi forniti dal Fornitore, nonché quelle ulteriori misure necessarie a garantire un livello di sicurezza adeguato al rischio. In particolare, il Fornitore si impegna ad implementare, applicare e tenere costantemente aggiornata ogni misura necessaria a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;

g) Il Fornitore è tenuto a tracciare le attività di trattamento dei dati personali svolte per conto della Società mediante apposito Registro del trattamento, redatto ai sensi dell'art. 30, par. 2 del Regolamento UE. Inoltre, tenuto conto della natura del trattamento e delle informazioni a disposizione, il Responsabile assiste la Società nel garantire il rispetto di tutti gli ulteriori obblighi previsti dal Regolamento UE e di seguito individuati:

   - art. 32. Sicurezza del trattamento;
   - art. 33. Notifica di una violazione dei Dati Personali all'autorità di controllo;
   - art. 34. Comunicazione di una violazione dei Dati Personali ai soggetti interessati;
   - art. 35. Valutazione d'impatto sulla protezione dei Dati Personali;
   - art. 36. Consultazione preventiva;

h) Il Fornitore, laddove tenuto alla nomina del Responsabile della Protezione dei Dati Personali ai sensi dell'art. 37 del Regolamento UE, si impegna a comunicare i dati di contatto del proprio Responsabile per la Protezione dei Dati Personali, provvedendo, altresì, ad informare la Società di ogni eventuale variazione con riguardo allo stesso.

3.1 Obblighi in tema di cooperazione e di informazione

Nell'ambito dei reciproci rapporti in ambito privacy, la Società e il Fornitore si devono impegnare reciprocamente ad agire secondo buona fede, nonché a collaborare per assicurare il rispetto della normativa applicabile in materia di trattamento dei dati personali, ivi incluse, a titolo puramente esemplificativo e non

esaustivo, quelle inerenti gli obblighi in materia di esercizio dei diritti privacy da parte dei soggetti interessati e di gestione degli incidenti sulla sicurezza che possano integrare violazioni dei dati personali rilevanti ai fini della normativa anzidetta. La Società ed il Fornitore devono collaborare, altresì, al fine di garantire la costante disponibilità di tutte le informazioni, relative al trattamento dei dati personali trattati, necessarie a dimostrare il rispetto della normativa applicabile in materia di trattamento dei dati personali, anche al fine di fornire, ove necessario, le anzidette informazioni all'Autorità Garante. In particolare, il Responsabile collabora con il Titolare affinché quest'ultimo dia riscontro alle richieste, relative al trattamento dei dati personali, avanzate dall'Autorità di Controllo; inoltre il Fornitore è tenuto a collaborare con la Società nelle ipotesi in cui quest'ultimo venga sottoposto ad una qualsiasi attività di controllo e verifica condotta dall'Autorità anzidetta, purché pertinente al trattamento dei dati personali svolto.

Il Fornitore informa spontaneamente la Società in merito a qualsiasi situazione ritenuta rilevante in materia di trattamento dei dati personali e di sicurezza e comunica, senza ingiustificato ritardo, tutte le informazioni espressamente richieste dal Titolare in relazione al trattamento dei dati personali svolto. In particolare, il Fornitore si impegna a fornire riscontro, in forma scritta, alle anzidette richieste entro dieci [10] giorni dal ricevimento delle richieste stesse.

Il Fornitore deve informare tempestivamente la Società di ogni comunicazione o richiesta ricevuta da un'Autorità di Controllo in relazione al trattamento dei dati personali trattati. In particolare, il Fornitore, nel caso in cui venga sottoposto ad una qualsiasi forma di verifica da parte dell'Autorità di Controllo o da parte di altra autorità nazionale o comunitaria, con riferimento al trattamento di dati personali, provvede, se consentito in base alla normativa applicabile, a informare per iscritto la Società senza ingiustificato ritardo e in ogni caso entro ventiquattro [24] ore dall'inizio della relativa attività di ispezione e controllo da parte dell'autorità.

Il Fornitore è tenuto ad informare, per iscritto e senza ingiustificato ritardo, la Società qualora ritenga che le istruzioni dallo stesso impartite con riguardo al trattamento si pongano in violazione della normativa applicabile in materia di trattamento dei dati personali. Inviata la relativa comunicazione alla Società, il Fornitore si astiene dal compimento delle operazioni di trattamento potenzialmente in contrasto con la normativa anzidetta, sino alla ricezione di nuove ed ulteriori istruzioni da parte della Società. Resta inteso che la Società potrebbe confermare le istruzioni inizialmente impartite, laddove escluda una violazione della normativa applicabile in materia di trattamento dei dati personali.

3.2 Ricorso ad ulteriori Subresponsabili del trattamento

Tipicamente, la Società, prendendo atto che, ai fini della compiuta esecuzione dei servizi, il Fornitore potrebbe dover avvalersi di subappaltatori, può autorizzare, il Fornitore a ricorrere ad eventuali Subresponsabili, fermo restando che, a tal fine, il Fornitore si deve impegnare a trasmettere alla Società, per iscritto e in ogni caso prima di procedere all'affidamento di specifiche attività o servizi agli eventuali Subresponsabili, apposita richiesta di autorizzazione.

In ogni caso, il Fornitore è tenuto al rispetto delle seguenti condizioni:

a) Informare la Società, senza ingiustificato ritardo e comunque prima dell'affidamento di specifiche attività o servizi ai subappaltatori, dell'identità dei Subresponsabili e comunicare, per iscritto e senza ingiustificato ritardo, ogni successiva modifica o aggiornamento dell'elenco dei Sub-Responsabili di cui si avvale, anche al fine di consentire alla Società di opporsi all'impiego di determinati Subresponsabili;

b) Stipulare con i Subresponsabili contratti che prevedano, in capo a questi ultimi, gli stessi obblighi previsti in capo al Fornitore stesso;

c) Svolgere, in fase di selezione dei Subresponsabili, un'adeguata *due diligence* al fine di constatare l'idoneità dei potenziali Subresponsabili a garantire il rispetto della normativa applicabile in materia di trattamento dei dati personali;

d) Fornire alla Società, previa sua richiesta, ogni informazione relativa alle politiche di protezione dei dati personali implementate dai Subresponsabili.

3.3 Trasferimenti di dati personali

Il Responsabile non può trasferire i dati personali trattati in considerazione dell'erogazione dei servizi al di fuori del territorio dell'UE o dello SEE.
Laddove dovesse venire in rilievo l'effettiva necessità di trasferire i dati personali ai fini della compiuta esecuzione dei servizi stessi, il trasferimento potrà essere consentito esclusivamente previa e specifica autorizzazione della Società in tal senso. A tal fine il Fornitore è tenuto a comunicare, per iscritto e senza ingiustificato ritardo e, in ogni caso, prima che il trasferimento stesso abbia luogo, ogni informazione rilevante con riguardo al trasferimento, anche al fine di consentire alla Società di rilasciare, se del caso, l'eventuale autorizzazione.
Parimenti, qualora le leggi nazionali o comunitarie impongano un trasferimento dei dati personali verso un Paese terzo o un'Organizzazione internazionale, il Fornitore sarà tenuto ad informare la Società in merito a tale obbligo giuridico. La relativa comunicazione dovrà essere effettuata, per iscritto e senza ingiustificato ritardo e, in ogni caso, prima che il trasferimento stesso abbia luogo. Il Fornitore è esonerato dall'obbligo di effettuare l'anzidetta comunicazione esclusivamente nell'ipotesi in cui la normativa *pro tempore* vigente ed applicabile vieti tale informazione per rilevanti motivi di interesse pubblico.
In entrambi i casi summenzionati il Fornitore garantisce che l'eventuale trasferimento dei dati personali, legalmente imposto o richiesto ai fini dell'erogazione dei servizi e comunque espressamente autorizzato dalla Società, avvenga sulla base dell'esistenza di una decisione di adeguatezza della Commissione Europea sul livello di protezione predisposto per i dati personali dal Paese terzo, ovvero sulla base di clausole contrattuali modello, debitamente adottate *ex* art. 46 del Regolamento UE, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento UE.

3.4 Esercizio dei diritti privacy

Il Fornitore è tenuto a collaborare con la Società, anche mediante l'adozione di specifiche misure tecniche ed organizzative, al fine di fornire il dovuto riscontro ai soggetti interessati che abbiano esercitato i propri diritti privacy ai sensi degli artt. 15 e ss. del Regolamento UE.
Inoltre il Fornitore provvede a comunicare alla Società ogni eventuale informazione idonea a dimostrare il rispetto degli obblighi previsti, a suo carico e nei confronti dei soggetti interessati, dalla normativa applicabile in materia di trattamento dei dati personali.
Laddove i soggetti interessati trasmettano le richieste di esercizio dei diritti privacy direttamente al Fornitore, quest'ultimo deve provvedere a darne tempestiva comunicazione scritta alla Società entro due [2] giorni dal ricevimento delle richieste stesse, nonché ad evadere le richieste senza ingiustificato ritardo e al più tardi entro un mese dal loro ricevimento, fornendo riscontro ai soggetti interessati esclusivamente previa autorizzazione scritta della Società.

3.5 Gestione delle violazioni di dati personali

Il Fornitore è tenuto ad informare la Società in merito al verificarsi di una violazione dei dati personali, ovvero di un incidente di sicurezza che incida sulla riservatezza, l'integrità e la disponibilità dei dati personali, comportandone, a titolo esemplificativo e non esaustivo, la distruzione, la perdita, la modifica, la divulgazione non autorizzata, ovvero l'accesso accidentale o illegale ai dati stessi. La comunicazione deve essere effettuata entro e non oltre le 48 ore dall'avvenuta conoscenza della violazione dei dati personali, scrivendo all'indirizzo e-mail databreach@formulaserviziallepersone.it e fornendo le seguenti informazioni:

- la natura della violazione dei dati personali, le categorie e il numero approssimativo dei soggetti interessati coinvolti, nonché le categorie e il numero approssimativo di registrazione dei dati in questione;
- il nome e i dati di contatto del Responsabile della protezione dei dati personali;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione al fine di porre rimedio alla violazione dei dati personali o al fine di attenuarne i possibili effetti negativi.

3.6 Restituzione e cancellazione dei dati personali

Il periodo di conservazione dei dati personali trattati deve coincidere, tipicamente, con la durata di erogazione dei servizi, salvo non sia diversamente previsto dalla Società o da specifici obblighi di legge. A tal fine, il Fornitore si deve impegnare, su indicazione della Società, a restituire o a cancellare i dati personali, nonché le eventuali copie dei medesimi, al termine dell'erogazione dei servizi o in un momento anteriore a quest'ultimo su richiesta espressa della Società.
Il Fornitore, di regola, è tenuto a provvedere alla cancellazione o alla restituzione dei dati personali senza ingiustificato ritardo e comunque non oltre 48 ore che decorrono dal momento della ricezione della richiesta della Società.

3.7 Attività di audit

La Società potrà disporre ed eseguire, anche tramite un terzo *auditor*, controlli e verifiche periodiche sulle operazioni di trattamento, nonché sull'adeguatezza delle misure tecniche e organizzative, ivi comprese le misure di sicurezza di cui all'art. 32 Regolamento UE, al fine di valutare la conformità delle attività poste in essere dal Fornitore alle istruzioni fornite per il trattamento e alla normativa applicabile in materia privacy.
Si precisa, altresì, che i controlli e le verifiche potranno includere anche le attività di ispezione presso le sedi in cui il Fornitore svolge le attività di trattamento.
Laddove, a seguito delle attività di controllo e di verifica, si dovesse ravvisare la violazione di quanto previsto dalla normativa nazionale e comunitaria ovvero dalle istruzioni ricevuto dalla Società, anche con riferimento alle misure tecniche ed organizzative e di sicurezza applicate, il Fornitore si deve impegnare a concordare con la Società e ad adottare, a proprie spese, ogni misura correttiva che si renda necessarie.