DISCIPLINARE PER LA PROTEZIONE DEI DATI PERSONALI APPLICATO DALLA SOCIETA’/TITOLARE:

CIRCOLO DIDATTICO STATALE "DON BOSCO"
VIA L.PIRANDELLO, 70
92024 CANICATTI' (AG)
Email: agee01100c@istruzione.it |
PEC: agee01100c@pec.istruzione.it |
Tel. 0922-832131
P. IVA 82002190849

PREMESSA
DISPOSIZIONI DI RIFERIMENTO
GLOSSARIO
Articolo 1 - Oggetto ed ambito di applicazione
Articolo 2 - L'accountability e il disciplinare privacy
Articolo 3 - Le finalità del trattamento dei dati personali
Articolo 4 - Il Titolare del trattamento dei dati personali
Articolo 5 - La protezione dei dati personali fin dalla progettazione e la protezione per impostazione
predefinita
Articolo 6 - I dati personali trattati
Articolo 7 - La valutazione di impatto sulla protezione dei dati e la consultazione preventiva con l'Autorità Garante Privacy
Articolo 8 - Il trattamento dei dati personali
Articolo 9 - Il trattamento di categorie particolari di dati personali
Articolo 11 - I diritti dell'interessato
Articolo 12 - Diritto di opposizione
Articolo 13 - Il diritto di accesso e il diritto alla riservatezza
Articolo 14 - Il registro delle attività di trattamento dei dati personali
Articolo 15 - I principi di sicurezza del trattamento
Articolo 16 - La comunicazione e diffusione dei dati personali
Articolo 17 - Le responsabilità del trattamento dei dati personali
Articolo 18 – I Delegati al trattamento
Articolo 19 - I Responsabili del trattamento dei dati personali
Articolo 20 - Gli interventi tecnici a cura di soggetti esterni
Articolo 21 - Gli autorizzati al trattamento dei dati personali
Articolo 22 - Gli amministratori di sistema
Articolo 23 - Il Data Protection Officer
Articolo 24 - Le misure di sicurezza
Articolo 25 - Le misure di sicurezza per i trattamenti di dati personali affidati ai Responsabili del trattamento dei dati personali
Articolo 26 - La tenuta in sicurezza dei documenti e archivi di titolarità
Articolo 27 - La violazione dei dati personali
Articolo 28 - I limiti alla conservazione dei dati personali
Articolo 29 - Il controllo a distanza
Articolo 30 - Attività di verifica e controllo dei trattamenti di dati personali
Articolo 31 - La formazione dei Delegati, Autorizzati e Amministratori di sistema
Articolo 32 - La disciplina delle misure del regolamento
Articolo 33 - Le norme transitorie e finali

PREMESSA

Alla luce dell'attuale quadro normativo, il nostro Istituto scolastico adotta il presente documento, denominato "Disciplinare per la protezione dei dati personali" (di seguito Disciplinare), che individua una serie di misure di sicurezza tecniche ed organizzative, finalizzate a proteggere i dati personali, delineando al contempo compiti e responsabilità di tutti coloro che trattano dati personali e contribuendo, altresì, ad implementare il sistema di ***accountability*** (responsabilizzazione) adottato dal nostro Istituto nella sua veste di Titolare del trattamento.

DISPOSIZIONI DI RIFERIMENTO

- Decreto Legislativo n. 196 del 2003 "Codice in materia di protezione dei dati personali";
- Decreto Legislativo n.101 del 2018 di adeguamento della normativa nazionale in materia di protezione dei dati personali alle disposizioni GDPR;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo n. 82 del 2005 "Codice dell'Amministrazione digitale";
- Legge n. 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- Decreto Legislativo n. 33 del 2013, "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".

GLOSSARIO

- «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un dato identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, genetica, psichica, economica, culturale o sociale;
- «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;
- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; Alla luce dell'attuale quadro normativo, la nostra società adotta il presente documento, denominato "Disciplinare per la protezione dei dati personali" (di seguito Disciplinare), che individua una serie di misure di sicurez za tecniche ed organizzative, finalizzate a proteggere i dati personali, delineando al contempo compiti e responsabilità di tutti coloro che trattano dati personali e contribuendo, altresì, ad implementare il sistema di ***accountability***
(responsabilizzazione) adottato dalla nostra società nella sua veste di Titolare del trattamento.
- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati utile per la valutazione di aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- «pseudonimizzazione»: il trattamento dei dati personali in una forma che impedisca l'identificazione dell'utente, a condizione che le informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti ad una persona fisica identificata o identificabile;
- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le

finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- «autorizzati»: persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- **«Interessato»**: persona fisica cui si riferiscono i dati personali;
- **«terzo»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del titolare o del responsabile;
- **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **«violazione dei dati personali»:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **«dati genetici»:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati biometrici»:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **«dati identificativi»:** i dati personali che permettono l'identificazione diretta dell'interessato;
- **«dati sensibili»:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati di salute non possono essere diffusi. I dati sensibili sono oggetto di comunicazione, anche verso soggetti pubblici, solo se prevista da disposizioni di legge o di regolamento;
- **«dato anonimo»:** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **«comunicazione»:** il dare conoscenza dei dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **«Autorità Garante della protezione dei dati personali»:** l'autorità pubblica indipendente deputata al controllo del rispetto della normativa vigente in materia di protezione dei dati personali.

ARTICOLO 1
OGGETTO ED AMBITO DI APPLICAZIONE L'ACCOUNTABILITY E IL DISCIPLINARE PRIVACY

Tali misure, riesaminate e aggiornate periodicamente, sono parte del presente documento, che include:
- il registro delle attività di trattamento dei dati personali;
- le regole di attribuzione delle responsabilità del trattamento dei dati personali;
- la documentazione relativa alle informative ed al rilascio delle autorizzazioni al trattamento dei dati;
- la documentazione relativa alle valutazioni preliminari d'impatto privacy; Il presente disciplinare si applica ai dati personali trattati dal nostro Istituto scolastico e ha lo scopo di garantire che il trattamento analogico, automatizzato o cartaceo di dati personali, effettuato anche per il tramite di soggetti autorizzati ai sensi degli articoli 28 e 29 del GDPR, avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché, della dignità delle persone, con particolare riferimento alla riservatezza ed all'identità personale, secondo le disposizioni vigenti in materia di protezione dei dati e in materia di amministrazione digitale.

ARTICOLO 2
L'ACCOUNTABILITY E IL DISCIPLINARE PRIVACY DELL'INL

Il Titolare adotta tutte le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato, così da assicurare il rispetto dei principi di liceità, correttezza e trasparenza nel trattamento dei dati personali e assicura l'adozione di adeguate e preventive misure di sicurezza, idonee ad evitare situazioni di rischio e di non conformità o di alterazione dei dati. Il Titolare mette in atto tutte le misure tecniche ed organizzative adeguate per garantire che il trattamento dei dati personali sia effettuato nel rispetto della normativa vigente, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento.

- le regolamentazioni, le procedure e le disposizioni operative adottate;
- la procedura di analisi dei rischi e il relativo documento di valutazione;
- le procedure di audit e verifica periodica del corretto trattamento dei dati personali;
- la procedura di gestione delle violazioni dei dati personali;
- la procedura di formazione continua dei Delegati al trattamento, Autorizzati al trattamento ed Amministratori di Sistema;
- la procedura di gestione delle istanze degli Interessati.

ARTICOLO 3
LE FINALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

L'Istituto svolge attività di trattamento di dati personali per il raggiungimento delle seguenti finalità:
- gestione del personale e dei collaboratori;
- gestione in materia di lavoro, assicurazione obbligatoria e legislazione sociale;
- gestione di tutela della salute e della sicurezza nei luoghi di lavoro
- tutela del proprio patrimonio;
- controllo e valutazione della propria attività;
- gestione clienti e fornitori;
- difesa dei propri diritti.
- gestione iscrizione alunni

ARTICOLO 4
IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

L'Istituto scolastico è il Titolare del trattamento dei dati personali, adotta tutte le misure tecniche ed organizzative atte a garantire che il trattamento dei dati personali sia effettuato conformemente alla normativa vigente. Nel caso in cui la scuola determini congiuntamente ad altri Titolari del trattamento le finalità e i mezzi del trattamento, assume la veste di Contitolare del trattamento, determinando in modo trasparente, congiuntamente con gli altri Contitolari, mediante un accordo interno scritto, le rispettive responsabilità in merito all'osservanza degli obblighi previsti dalla normativa vigente, con particolare riguardo all'esercizio dei diritti dell'Interessato. L'Istituto, tramite il Data Protection Officer (di seguito DPO), di cui all'art.24 del presente Regolamento, nei casi previsti dalla legge, provvede a:
- assolvere ogni obbligo di comunicazione, interpello o notificazione all'Autorità Garante per la Privacy;
- cooperare, su richiesta, con l'Autorità Garante per la Privacy nell'esecuzione dei suoi compiti;
- richiedere a tale Autorità ogni necessaria autorizzazione al trattamento dei dati personali, ove necessaria;
- adottare, per quanto di competenza, le misure necessarie a garantire la protezione dei dati personali, anche per quanto riguarda il processo di digitalizzazione;
- adottare una procedura di valutazione d'impatto privacy (Data Privacy Impact Assessment) per le attività di trattamento dati al fine di attivare e mantenere aggiornato il Registro delle attività di trattamento effettuate all'interno dal Titolare di cui al successivo articolo 14;
- assicurare l'informazione e la formazione del personale sul tema della tutela della riservatezza dei dati personali;
- nominare i Delegati, gli Autorizzati e i Responsabili del trattamento di dati personali impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali.

Il Titolare del trattamento è tenuto ad effettuare, nei confronti di tutti coloro che svolgono per suo conto

attività di trattamento, le verifiche ed i controlli atti a garantire il rispetto degli obblighi previsti dalle disposizioni vigenti in materia.

ARTICOLO 5
LA PROTEZIONE DEI DATI PERSONALI FIN DALLA PROGETTAZIONE E LA PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, come la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, o la minimizzazione e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
La società adotta ogni misura tecnica e organizzativa adeguata per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

ARTICOLO 6
I DATI PERSONALI TRATTATI

I dati personali sono trattati utilizzando documenti cartacei o informatizzati, soltanto qualora siano essenziali e necessari allo svolgimento delle attività istituzionali indicate dal precedente art. 3 e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati pseudonimizzati, fatto salvo in ogni caso il diritto all'anonimato nei casi previsti da normative vigenti.
La società adotta ogni misura tecnica e organizzativa adeguata per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. La società tratta i dati di tipo personale e sensibile relativi a: - cittadini/utenti, loro familiari e/o accompagnatori; - personale in rapporto di dipendenza, convenzione o collaborazione; - clienti e fornitori. I dati personali trattati dalla società nelle forme e nei limiti di quanto previsto dalla normativa vigente sono raccolti presso l'interessato, presso terzi, altri enti e amministrazioni pubbliche e/o presso
pubblici registri.

ARTICOLO 7
LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E LA CONSULTAZIONE PREVENTIVA CON L'AUTORITÀ GARANTE PRIVACY

La società assicura che sia effettuata una valutazione di impatto preliminare al trattamento dei dati personali, qualora necessario, del DPO. La valutazione, disciplinata dalla società con apposita procedura, viene effettuata nei casi e nei modi previsti dalle disposizioni vigenti, al fine di valutare i rischi del trattamento, le misure previste per contenerli, le misure di sicurezza e i meccanismi atti a garantire la protezione dei dati personali e dimostrare la conformità alle norme vigenti, tenuto conto dei diritti degli interessati e delle finalità del trattamento. Nel caso di attivazione di un nuovo trattamento di dati personali, il DPO ed avvalendosi delle ulteriori risorse necessarie, effettua l'apposita valutazione preliminare di impatto, da conservarsi agli atti e sottoporre a riesame periodico qualora insorgano variazioni del rischio relativo al trattamento. Qualora la valutazione d'impatto sulla protezione dei dati evidenzi un rischio elevato, prima di procedere al trattamento, la società consulta l'Autorità Garante Privacy per il tramite del proprio DPO. La società attiva, inoltre, tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche già individuate dall'Autorità Garante Privacy per il corretto trattamento dei dati, in modo particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi integrati.

ARTICOLO 8
IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento effettuato da soggetti a ciò non preventivamente formati e formalmente autorizzati è illecito.
I Delegati al trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

I Delegati, gli Autorizzati e gli Amministratori di Sistema sono legittimati all'esecuzione delle operazioni di trattamento strettamente necessarie al perseguimento delle finalità alle quali lo specifico trattamento dei dati personali è preordinato.
I Delegati sono tenuti a comunicare dati personali e/o sensibili agli altri Delegati al trattamento solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati pseudonimizzati, anonimi o aggregati.
I dati personali possono essere oggetto di conservazione, sia analogica che digitale, solo per il tempo previsto dalla normativa vigente e successivamente sottoposti a scarto d'archivio e distruzione. La società assicura che sia effettuata una valutazione di impatto preliminare al trattamento dei dati personali, avvalendosi anche , qualora necessario del DPO. La valutazione, disciplinata dalla società con apposita procedura, viene effettuata nei casi e nei modi previsti dalle disposizioni vigenti, al fine di valutare i rischi del trattamento, le misure previste per contenerli, le misure di sicurezza e i meccanismi atti a garantire la protezione dei dati personali e dimostrare la conformità alle norme vigenti, tenuto conto dei diritti degli interessati e delle finalità del trattamento. Nel caso di attivazione di un nuovo trattamento di dati personali, il Titolare e il DPO avvalendosi delle ulteriori risorse necessarie, effettua l'apposita valutazione preliminare di impatto, da conservarsi agli atti e sottoporre a riesame periodico qualora insorgano variazioni del rischio relativo al trattamento. Qualora la valutazione d'impatto sulla protezione dei dati evidenzi un rischio elevato, prima di procedere al trattamento, la società consulta l'Autorità Garante Privacy per il tramite del proprio DPO. La società attiva, inoltre, tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche già individuate dall'Autorità Garante Privacy per il corretto trattamento dei dati, in modo particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi integrati. All'interno della società sono individuati i ruoli e i compiti dei soggetti autorizzati a trattare i dati personali, attività consentita esclusivamente a Delegati, Autorizzati, Responsabili del trattamento, eventuali Sub-Responsabili del trattamento e Amministratori di Sistema. Il trattamento può avere ad oggetto i soli dati essenziali e necessari ad assolvere le finalità e deve essere attuato in modo da assicurare il rispetto dei diritti e della dignità dell'interessato.
In particolare, i Delegati e i Responsabili del trattamento, con riguardo alla gestione, protezione e manutenzione dei sistemi informativi e dei programmi informatici, dovranno assicurare al Titolare del trattamento che tali sistemi e programmi siano pre-configurati, in ossequio al già citato principio della "privacy per impostazione predefinita", riducendo al minimo l'utilizzazione di dati personali, così da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità di pseudonimizzazione che permettano di identificare l'interessato solo in caso di necessità.
I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
I trattamenti di dati effettuati utilizzando le banche dati di più Titolari, sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

ARTICOLO 9
IL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

L'Istituto tratta dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita o all'orientamento sessuale della persona soltanto se il trattamento è necessario:
- per assolvere agli 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 accertare, esercitare o difendere un diritto;
- per eventuali motivi di interesse pubblico rilevante, proporzionato alla finalità perseguita;
- per tutelare i diritti fondamentali e gli interessi dell'interessato;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente.

ARTICOLO 10
LE INFORMAZIONI ALL'INTERESSATO

L'Istituto adotta le informazioni sul trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
Le informazioni sul trattamento dei dati personali riportano gli elementi essenziali previsti dalla normativa vigente relativamente a:
- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del DPO;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le modalità di trattamento dei dati personali; La società tratta dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita o all'orientamento sessuale della persona

soltanto se il trattamento è necessario:
- l'obbligatorietà o meno del conferimento dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'individuazione di coloro ai quali i dati personali possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- le modalità di esercizio dei diritti di accesso in base alle disposizioni vigenti;
- l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali e la rettifica del trattamento, ovvero di opporsi al loro trattamento degli stessi;
- il diritto di proporre reclamo all'Autorità Garante Privacy;
- le ipotesi in cui la comunicazione di dati personali è un obbligo legale o contrattuale, oppure è un requisito necessario per la conclusione di un contratto, e le ipotesi in cui l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e in tali casi le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste per l'interessato;
- l'informazione all'interessato circa la fonte da cui hanno origine i dati personali nel caso in cui non siano stati ottenuti presso l'interessato stesso e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

ARTICOLO 11
I DIRITTI DELL'INTERESSATO

L'interessato può contattare la società o il DPO per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei propri diritti, anche al fine di avere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, nonché, al fine dell'accesso ai dati personali e alle seguenti informazioni:
- finalità del trattamento;
- categorie di dati personali trattate;
- destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; L'informativa all'Interessato viene resa, anche per estratto, tramite l'affissione di appositi manifesti o la consegna di appositi documenti nei locali di accesso all'utenza, utilizzando i sistemi Internet ed Intranet, dove sono evidenziate le azioni poste in essere all'interno della società in attuazione della normativa sulla riservatezza dei dati. L'informativa sul trattamento dei dati personali non viene rilasciata all'Interessato, da parte della società, nel caso in cui questi disponga già delle relative informazioni, o nel caso in cui comunicarle risulti impossibile ovvero implicherebbe uno sforzo sproporzionato da parte dell'amministrazione.

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità di detto interessato. L'interessato può contattare la società o il DPO per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei propri diritti, anche al fine di avere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, nonché, al fine dell'accesso ai dati personali e alle seguenti informazioni:

- periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- diritto alla rettifica o cancellazione dei dati personali o alla limitazione del trattamento dei dati personali che lo riguardano o di opposizione al loro trattamento;
- diritto di proporre reclamo all'Autorità Garante Privacy;
- informazioni disponibili sulla origine dei dati che non siano raccolti presso l'interessato stesso;
- esistenza di un processo decisionale automatizzato, compresa profilazione e informazioni significative sul sistema utilizzato.

L'Interessato, nell'esercizio dei diritti sopra riportati, può conferire per iscritto delega o procura a persone fisiche o ad associazioni.
Se riferiti a dati personali concernenti persone decedute, i diritti di cui al comma 1 possono essere esercitati da chiunque vi abbia un interesse giuridicamente rilevante documentato nelle forme di legge, anche mediante delega o procura a persone fisiche o ad associazioni, conferita per iscritto e nelle modalità di legge.

ARTICOLO 12
DIRITTO DI OPPOSIZIONE

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei propri dati personali. A seguito dell'esercizio di tale diritto, il Titolare si astiene dall'ulteriore trattamento, salvo che dimostri l'esistenza di motivi legittimi cogenti che prevalgono sugli interessi, diritti e libertà dell'interessato, ovvero dimostri la necessità di procedere comunque al trattamento ai fini dell'accertamento, esercizio o difesa di un diritto in sede giudiziaria.

ARTICOLO 13
IL DIRITTO DI ACCESSO E IL DIRITTO ALLA RISERVATEZZA

Il Titolare, nel rispetto della normativa in vigore, gestisce le istanze dell'Interessato, circa il diritto di accedere ai documenti. Al riguardo, ulteriori specifiche indicazioni agli operatori sono contenute nelle altre istruzioni operative adottate.
Il DPO, o il Titolare, avviano il procedimento, disciplinato con apposita procedura, avvalendosi necessariamente dell'apporto e della collaborazione del Delegato al trattamento dei dati di competenza e degli Amministratori di Sistema interessati. L'interessato ha il diritto di ottenere dalla società, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano e l'integrazione dei dati personali incompleti, anche sulla base di una dichiarazione integrativa; a tal fine, avanzare specifica istanza al DPO o all'Ufficio di Staff.

ARTICOLO 14
IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI

Il Titolare, individua, come elementi fondamentali delle politiche di protezione dei dati personali, l'analisi dei trattamenti e la distribuzione dei compiti e delle responsabilità attribuite a coloro che sono incaricati di trattare dati personali; provvede, inoltre, alla rilevazione dei trattamenti dei dati personali, suddivisi per tipologia e per struttura organizzativa e ogni altro elemento necessario ad individuare le responsabilità relative al loro trattamento.
Il Titolare, tiene un registro delle attività di trattamento dei dati personali di riferimento, costantemente aggiornato, che evidenzia i diversi livelli di responsabilità attribuiti nell'ambito del trattamento ai Responsabili, ai Sub-responsabili, ai Delegati, agli Autorizzati e agli Amministratori di Sistema e che contiene le seguenti informazioni:
- i trattamenti di dati personali per ognuno dei soggetti sopra elencati;
- il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento e del Data Protection Officer;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- gli eventuali trasferimenti di dati personali verso un paese terzo e la documentazione delle garanzie adeguate;

- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- la descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali oggetto di trattamento.

Il Registro è tenuto sia in forma scritta che in formato elettronico e viene messo, su richiesta, a disposizione dell'Autorità Garante Privacy.

I Responsabili esterni e Sub-Responsabili del trattamento che trattano dati personali su delega del Titolare devono annotare il trattamento delegato nelle forme ed ai sensi del comma 2 dell'articolo 30 del GDPR.

ARTICOLO 15
I PRINCIPI DI SICUREZZA DEL TRATTAMENTO

Il Titolare, adotta misura idonee ad assicurare e documentare che il trattamento dei dati personali sia effettuato con modalità tali da preservarne l'integrità e la confidenzialità, nel rispetto di adeguate misure di sicurezza.

A riguardo, attiva le necessarie risorse organizzative, tecnologiche e finanziarie affinché il trattamento dei dati personali sia conforme alle disposizioni in materia di protezione dei dati e di amministrazione digitale nell'osservanza dei seguenti principi:

· «liceità, correttezza e trasparenza», i dati sono trattati in modo lecito, corretto e trasparente;

· «limitazione della finalità», i dati sono raccolti per finalità determinate, esplicite e legittime, e trattati in modo che non sia incompatibile con tali finalità;

· «minimizzazione dei dati», i dati debbono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

· «esattezza», i dati devono essere esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

· «limitazione della conservazione», i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, salvo che vengano conservati per periodi più lunghi ai soli fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

· «integrità e riservatezza», i dati sono trattati in maniera da garantire, mediante idonee misure tecniche e organizzative, un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non p autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

· «responsabilizzazione», i dati sono trattati nel pieno rispetto della normativa vigente.

ARTICOLO 16
LA COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

La comunicazione dei dati personali all'esterno è effettuata in forma scritta o telematica esclusivamente alla Pubblica Amministrazione e altri soggetti di natura pubblica e privata, in esecuzione di obblighi derivanti da normative vigenti.

Il Titolare, assicura che la comunicazione o l'interscambio di dati personali per l'espletamento delle finalità istituzionali sia effettuata soltanto nei limiti del principio di necessità, osservando le disposizioni del presente regolamento e delle relative misure di sicurezza e la diffusione dei dati personali e sensibili è consentita soltanto per adempiere ad obblighi previsti dalle normative vigenti e nelle forme da queste previste.

ARTICOLO 17
LE RESPONSABILITÀ DEL TRATTAMENTO DEI DATI PERSONALI

I Delegati, i Responsabili e i Sub-Responsabili del trattamento designati dal Titolare;

- trattano i dati personali conformemente alle istruzioni impartite dallo stesso;
- mettono a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e collaborano alle attività di revisione e alle attività di controllo interno;
- informano il Titolare e il DPO in ordine a ogni eventuale difformità alla normativa vigente, anche mediante comunicazione via mail.

ARTICOLO 18
I DELEGATI AL TRATTAMENTO

La funzione di Delegato al trattamento dei dati personali è attribuibile all'amministratore.
Il Delegato é designato dal Titolare con apposito atto formale, accompagnato da puntuali indicazioni operative per il corretto assolvimento dei compiti in materia di protezione dei dati, da notificarsi per iscritto al Delegato.
L'elenco dei Delegati al trattamento dei dati è tenuto in raccordo con il DPO.
Il Titolare, tramite l'Ufficio competente, conserva nel proprio sistema documentale la copia degli atti di designazione a Delegato al trattamento dei dati personali.
Il Delegato al trattamento dei dati personali, relativamente al proprio settore di competenza, risponde al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale; riferisce periodicamente in ordine alle modalità di svolgimento dei compiti assegnati; verifica che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, rispondano ai principi di necessità, pertinenza e non eccedenza, segnalando all'Ufficio di Staff eventuali situazioni di potenziale rischio.
Il Delegato al trattamento dei dati è dotato di autonomia gestionale ed organizzativa per il trattamento dei dati di propria competenza ed è tenuto ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione delle prestazioni e dei servizi in favore del titolare del dato.
Sulla base della modulistica appositamente predisposta dal Titolare, il Delegato designa formalmente gli Autorizzati del trattamento, fornendo loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento dei dati personali e vigila sul rispetto di tali istruzioni, anche attraverso verifiche periodiche.
Il Delegato al trattamento dei dati personali compie tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza, sicurezza e protezione dei dati relativamente ai trattamenti loro assegnati e, in particolare, è tenuto all'osservanza delle misure di sicurezza e delle altre precauzioni adottate, e delle ulteriori linee guida sulla riservatezza dei dati, la protezione delle informazioni e sull'amministrazione digitale.
Ha inoltre il compito di:
- designare, in forma scritta, gli Autorizzati del trattamento dei dati personali, secondo livelli differenziati e profili omogenei;
- adottare le misure di sicurezza dei dati personali, in base alle indicazioni impartite;
- curare la diffusione delle norme, delle linee guida e di ogni altra disposizione impartita dal Titolare fra gli Autorizzati del trattamento dei dati;
- adottare ulteriori istruzioni interne e indicazioni di comportamento per il personale e per gli utenti;
- collaborare con il Titolare e il DPO;
- verificare l'esattezza, l'aggiornamento, la pertinenza e la congruità dei dati, in rapporto all'attività svolta;
- effettuare, limitatamente all'ambito e agli aspetti di competenza, l'analisi dei rischi afferenti al trattamento dei dati e alla conservazione dei medesimi;
- verificare periodicamente il corretto trattamento dei dati personali da parte degli Autorizzati al trattamento;
- segnalare al Titolare l'inizio o la cessazione di trattamenti di dati personali e della cancellazione di dati personali, al fine di permettere l'aggiornamento del Registro delle attività di trattamento dei dati personali;
- trasmettere al Titolare, entro il 31 gennaio di ogni anno, una relazione sulle misure di sicurezza adottate, sulle modalità di trattamento dei dati e sulle eventuali criticità residue al 31 dicembre dell'anno precedente.

ARTICOLO 19
I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare, designa Responsabili del trattamento dei dati personali i soggetti a cui sono delegate attività di propria pertinenza o attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comunque comportano il trattamento dei dati personali.
Il Titolare, designa quali Responsabili del trattamento dei dati personali esclusivamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.

Il Responsabile del trattamento dei dati personali non può delegare, neppure in parte, ad altri soggetti denominati Sub-Responsabili, senza previa autorizzazione scritta del Titolare i trattamenti di dati personali che gli sono stati affidati.
Il Titolare, designa i Responsabili del trattamento attraverso uno specifico atto che indichi la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.
Tale atto prevede in particolare, che il Responsabile del trattamento deve:
- trattare i dati personali soltanto su istruzione documentata del Titolare;
- garantire che i dati trattati siano sottoposti al vincolo di riservatezza;
- adottare tutte le misure di sicurezza indicate dal Titolare e le ulteriori misure tecniche e organizzative capaci di garantire ai dati oggetto di trattamento un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, natura, oggetto, contesto e finalità del trattamento, rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- tenere conto della natura del trattamento, assistere il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfarne l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato e garantire il rispetto degli obblighi di legge, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
- cancellare o restituire, su indicazione del Titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento;
- mettere a disposizione del Titolare, le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuire alle attività di controllo, revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi autorizzato.
Nel caso in cui il Responsabile del trattamento, previa specifica autorizzazione scritta del Titolare, ricorra a un Sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto della scrivente società, questi è parimenti responsabile e tenuto al rispetto di quanto previsto dal presente articolo. In tutti gli atti che disciplinano rapporti con i soggetti di cui al precedente comma (contratti, convenzioni, scritture private, conferimenti, etc.) si dovrà rimandare alla successiva designazione a responsabile del trattamento.

ARTICOLO 20
GLI INTERVENTI TECNICI A CURA DI SOGGETTI ESTERNI

I soggetti esterni che, in forza di un rapporto contrattuale con il Titolare esercitino attività di manutenzione su apparecchiature utilizzate per il trattamento o la registrazione di dati devono fornire idonea garanzia del rispetto delle misure di sicurezza previste dalla normativa vigente.
Il Delegato che commissiona la manutenzione di apparecchiature utilizzate per il trattamento dei dati personali, anche nel caso in cui dette apparecchiature ne permettono il trattamento da parte di soggetti esterni non vincolati al Titolare, è tenuto a vigilare, anche a mezzo dei propri collaboratori, su ogni intervento tecnico operato dagli esecutori per tutta la durata del servizio stesso.
Preliminarmente alla stipula di ogni nuovo contratto di manutenzione, il Delegato competente provvede a richiedere al soggetto esterno le garanzie previste dalla normativa in materia di protezione dei dati personali dando altresì indicazione delle specifiche esigenze di sicurezza.

ARTICOLO 21
GLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Gli Autorizzati al trattamento dei dati personali effettuano le operazioni di trattamento di dati personali e/o sensibili su designazione del Delegato, che li nomina tra i dipendenti e i collaboratori che, a qualsiasi titolo, su mandato del Titolare stesso, prestino la loro opera, anche in via temporanea.
La designazione è fatta con apposito atto che costituisce l'unico presupposto di liceità per il trattamento dei dati personali e deve indicare la data di inizio e fine dell'attività (se prevista), i dati personali/sensibili relativi all'attività svolta, le indicazioni sul corretto uso dei dati, in special modo afferente al profilo della sicurezza e le direttive vigenti sulla protezione dei dati trattati.
Il Delegato è tenuto a comunicare tempestivamente, via mail e senza ritardo, la data di cessazione dell'incarico.

Gli Autorizzati al trattamento dei dati personali:
- qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata ed è fatto loro assoluto divieto di cedere la propria password ad altri;
- sono responsabili della custodia dei documenti cartacei loro affidati per l'esercizio delle loro funzioni e hanno l'obbligo di restituirli al termine delle operazioni affidate.
Sono da considerarsi soggetti autorizzati al trattamento dei dati anche i dipendenti e i collaboratori del Responsabile o Sub-Responsabile del trattamento.

ARTICOLO 22
GLI AMMINISTRATORI DI SISTEMA

Il Titolare, designa tra gli Autorizzati al trattamento dei dati personali i propri Amministratori di sistema, con un apposito atto corredato di specifiche istruzioni operative, la cui copia viene conservata presso l'Ufficio di Staff.
In caso di nuove richieste di credenziali per l'accesso alle procedure informatiche agli Amministratori di sistema, i Delegati dovranno inoltrare agli stessi l'atto formale di designazione.
I Responsabili e Sub-Responsabili del trattamento dei dati, cui sono state delegate competenze di gestione e protezione dei sistemi informativi e delle risorse hardware e software del Titolare, designano e coordinano l'attività degli Amministratori di Sistema e vigilano sugli adempimenti in materia di protezione dei dati. Sono pertanto tenuti ad assolvere a tutte le misure previste dalla normativa vigente in tema di Amministratore di Sistema ed a trasmettere al Titolare del trattamento, entro il mese di gennaio di ogni anno solare, le informazioni relative alle nomine, le ulteriori misure adottate e la copia della relativa documentazione.

ARTICOLO 23
IL DATA PROTECTION OFFICER

Il Titolare, designa un Responsabile della protezione dei dati o Data Protection Officer.
Il DPO, che può essere un dipendente del Titolare o assolvere i suoi compiti in base a un contratto di servizi, è designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere ai compiti individuati dalla normativa vigente.
Il Titolare pubblica i dati di contatto del DPO sul proprio sito, comunicandoli, altresì, all'Autorità Garante Privacy e fornisce allo stesso tutte le risorse necessarie per assolvere ai suoi compiti.
Il DPO attiva tutte le misure per favorire l'osservanza del presente disciplinare e delle altre disposizioni vigenti relative alla protezione dei dati ed ha i seguenti compiti:
- riferire, direttamente al Titolare sulle problematiche relative alla protezione dei dati personali;
- informare e fornire consulenza ai Delegati ed Autorizzati al trattamento dei dati personali in merito agli obblighi derivanti dalla normativa vigente in materia di protezione dei dati;
- sorvegliare l'osservanza del presente regolamento e delle altre disposizioni vigenti relative alla protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione dei Delegati e degli Autorizzati al trattamento e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- predisporre, anche su iniziativa del Titolare e in stretto raccordo con l'Ufficio di Staff, la modulistica, le linee guida, procedure, disposizioni operative, registri e policy necessari a rendere operative le indicazioni di legge e del presente regolamento;
- cooperare e fungere da punto di contatto per l'Autorità Garante Privacy per tutte le questioni connesse al trattamento dei dati personali, consultandola quando necessario.
Nell'eseguire i propri compiti il Data Protection Officer considera debitamente i rischi inerenti al trattamento dei dati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

ARTICOLO 24
LE MISURE DI SICUREZZA

Il Titolare e i Responsabili del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati.

Questi, 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, mettono in atto misure tecniche e organizzative confacenti per garantire un livello di sicurezza adeguato al rischio.
I Delegati al trattamento collaborano con il Titolare, adottando le misure loro indicate e vigilano sulla loro osservanza da parte degli Autorizzati.
Tali misure comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente disponibilità e accesso dei dati personali in caso di incidente;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Tutti coloro che trattano dati per conto del Titolare possono trattare dati personali solo se autorizzati e istruiti in tal senso dallo stesso.
L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento di dati per il quale l'incaricato del Titolare è stato precedentemente designato quale Autorizzato al trattamento ed è consentito soltanto utilizzando apposite credenziali di autorizzazione composte da password gestite in conformità alle regole tecniche di sicurezza.
La password è strettamente personale e, a nessun titolo, può essere comunicata a terzi e della sua riservatezza risponde personalmente il singolo Autorizzato al trattamento dei dati personali.
Il Delegato al trattamento dei dati è tenuto a comunicare agli Amministratori di Sistema e all'Ufficio di Staff la data di cessazione dell'incarico al trattamento dei dati da parte dei suoi collaboratori.
Spetta ad ogni Delegato comunicare all'Ufficio di Staff e all'Amministratore di Sistema gli aggiornamenti e le variazioni relative al personale (cessazioni, sostituzioni, incarichi, aspettative, assenze prolungate per almeno 180 gg, trasferimenti, ecc.) che comportano una modifica al sistema delle autorizzazioni al trattamento dei dati personali.
Il Titolare, adotta, entro il 30 giugno di ogni anno, un piano di audit al fine di:

- individuare le misure adeguate per elevare lo standard di sicurezza dei dati anche sulla base dell'analisi dei rischi;
- rappresentare la distribuzione dei compiti e delle responsabilità del trattamento dei dati;
- programmare l'attività di formazione degli Autorizzati, dei Delegati al trattamento e Amministratori di Sistema al fine di un utilizzo consapevole delle informazioni;
- evidenziare le misure che il Titolare ha adottato nel tempo per proteggere i dati personali a sua disposizione e il piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Il piano di audit è predisposto dall'Ufficio di Staff di concerto con il DPO e con il supporto del Servizio informatico, sulla base delle informazioni trasmesse dai Delegati e dai Responsabili del trattamento dei dati, e dagli Amministratori di sistema.
Entro il 31 gennaio di ogni anno, i Delegati al trattamento dei dati devono inviare all' Ufficio di Staff una relazione annuale sul loro operato, che deve evidenziare:

- l'attività svolta e le misure di sicurezza adottate;
- le carenze strutturali e organizzative;
- le specifiche necessità formative necessarie per l'attuazione delle disposizioni sulla riservatezza;
- le criticità di sicurezza riscontrate;
- le contromisure di cui si propone l'attivazione.

ARTICOLO 25
LE MISURE DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI AFFIDATI AI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

I Responsabili del trattamento sono tenuti ad assicurare al Titolare del trattamento di aver adottato, prima di

effettuare qualsiasi attività di trattamento di dati, ogni misura di sicurezza prevista dalla normativa vigente in tema di protezione di dati e amministrazione digitale.
Tali soggetti sono comunque tenuti ad assicurare il rispetto delle specifiche istruzioni operative impartite dal Titolare per la tenuta in sicurezza dei dati oggetto di affidamento e garantire di aver attivato ogni altra misura idonea alla protezione dei dati loro affidati.
Tali Responsabili sono tenuti ad inviare all'Ufficio di Staff, entro il 31 gennaio di ogni anno, una relazione dettagliata nella quale sono evidenziate:
- l'attività svolta e le misure di sicurezza adottate;
- l'elenco delle risorse hardware e software disponibili;
- le procedure di continuità operativa ed emergenza adottate;
- le misure di recupero da data- breach adottate;
- le misure di back-up del sistema informativo del Titolare e di contenimento dei virus informatici adottate, comprese quelle di conservazione sostitutiva;
- le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita/manomissione del patrimonio informativo gestito;
- le misure adottate per la cifratura, o la separazione dei dati relativi alla salute;
- le misure adottate per la gestione delle disposizioni in tema di Amministratori di Sistema, rimettendo al riguardo anche la relativa documentazione;
- le verifiche periodiche sul mantenimento in sicurezza che sono state adottate, con la relativa documentazione.

Nel caso in cui, nello svolgimento delle attività di trattamento, il Responsabile del trattamento utilizzi strumenti informatici propri, è tenuto ad attestare con una propria dichiarazione scritta di assicurare la protezione dei dati affidati dal Titolare attraverso specifiche misure adeguate di sicurezza e di non aver affidato alcune fasi del trattamento a soggetti terzi, salvo che il Titolare non abbia autorizzato la nomina di questi come Sub-responsabili del trattamento dei dati personali.
Qualora, al contrario, il Responsabile del trattamento utilizzi strumenti informatici forniti dal Titolare, è tenuto a trasmettere copia degli atti di designazione degli Autorizzati all'Ufficio di Staff, che provvederà ad attivare le procedure necessarie al rilascio delle relative credenziali di accesso.
Il mancato rispetto da parte del Responsabile del trattamento di misure di sicurezza adeguate a contenere o prevenire rischi che possono riguardare i dati oggetto dell'affidamento può costituire titolo per la rescissione del rapporto sottostante e per un'eventuale istanza del risarcimento del danno.

ARTICOLO 26
LA TENUTA IN SICUREZZA DEI DOCUMENTI E ARCHIVI DEL TITOLARE

Gli archivi, cartacei e digitali, che custodiscono i dati di cui è titolare del trattamento la scrivente società, devono essere collocati in locali non esposti a rischi ambientali, in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo del Titolare in tema di Continuità Operativa, Conservazione Sostitutiva e Disaster Recovery. La documentazione archiviata, anche digitalmente, che riporta dati personali è conservata per il tempo previsto dalla legge e poi sottoposta a scarto di archivio o cancellata definitivamente.
Il Delegato al trattamento individua, attenendosi alle indicazioni del DPO ed alle disposizioni del Titolare, i criteri necessari a garantire l'accesso controllato ai locali e l'accesso selezionato ai dati, mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio degli Archivi medesimi.
I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici) sono conservati e custoditi con le modalità indicate per gli archivi cartacei nei modi e termini previsti dalla normativa vigente.
L'accesso agli archivi cartacei della società è formalmente autorizzato da parte dei Delegati al trattamento e, per gli archivi digitali, da parte dell'Amministratore di Sistema. Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Delegato al trattamento dei dati di competenza, che deve assicurarne la riservatezza, la protezione e l'integrità per tutto il tempo in cui ne mantiene la disponibilità.
Relativamente agli archivi informatizzati di dati, facendo seguito alle disposizioni vigenti in tema di protezione dati e amministrazione digitale ed avvalendosi del DPO, e dei Delegati e Autorizzati al trattamento dei dati e degli Amministratori di Sistema, il Titolare adotta idonee procedure di:
- salvataggio periodico degli archivi di dati personali;

- misure di contenimento dei virus informatici;
- disaster recovery;
- continuità operativa;
- conservazione sostitutiva.

ARTICOLO 27
LA VIOLAZIONE DEI DATI PERSONALI

Ogni Delegato o Autorizzato, così come il Responsabile al trattamento dei dati personali, è tenuto a informare, senza ingiustificato ritardo e anche per il tramite dell'Ufficio di Staff, il Titolare o il DPO dell'ipotesi di una violazione dei dati personali, fornendo la massima collaborazione al fine di soddisfare le indicazioni degli articoli 33 e 34 del GDPR. Ogni Interessato, può effettuare la segnalazione al Titolare o al DPO Ufficio di Staff di un possibile caso di una violazione dei dati personali. In tali casi, il Titolare avvia le necessarie procedure, se del caso avvalendosi della collaborazione dei Responsabili del trattamento.
Il Titolare provvede a notificare la violazione all'Autorità Garante Privacy, per il tramite del Data Protection Officer, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati. La notifica non effettuata entro 72 ore è corredata dei motivi del ritardo.
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente.
La notifica della violazione dei dati personali deve:
- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il Titolare del trattamento documenta qualsiasi violazione dei dati personali in un apposito registro delle violazioni di dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto delle indicazioni di legge.

ARTICOLO 28
I LIMITI ALLA CONSERVAZIONE DEI DATI PERSONALI

Il Titolare, assicura l'adozione di apposite misure e procedure attraverso le quali:
- si proceda alla distruzione dei documenti analogici e digitali, una volta terminato il limite minimo di conservazione dei documenti e dei dati in questi riportati;
- siano smaltiti gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile l'accesso ad alcun dato personale di cui è titolare la scrivente società;
sia effettuato il riutilizzo di apparati di memoria o hardware con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare la scrivente società

ARTICOLO 29
IL CONTROLLO A DISTANZA

Ad ogni sistema di controllo a distanza, degli Interessati e/o del lavoratore, il Titolare, applica il principio di proporzionalità tra mezzi impiegati e fini perseguiti, nel rispetto delle disposizioni vigenti e delle ulteriori direttive dell'Autorità Garante per la protezione dei dati personali.
Il Titolare comunque garantisce il rispetto della disciplina del divieto di controllo a distanza del lavoratore, così come prevista dalla normativa di riferimento, ivi compreso il rispetto degli accordi con le rappresentanze sindacali della società, adottando i conseguenti regolamenti applicativi.

Per tutti i sistemi di controllo attivati dal Titolare, questo deve assicurare l'effettività delle misure di tutela degli interessati e dei lavoratori, in particolare per quanto riguarda l'erogazione di specifica informativa e la piena trasparenza delle caratteristiche, finalità e modalità del controllo operato.

ARTICOLO 30
ATTIVITÀ DI VERIFICA E CONTROLLO DEI TRATTAMENTI DI DATI PERSONALI

Il Titolare, individua modalità attraverso cui si svolgono le attività di verifica e controllo, anche periodico, del rispetto delle misure di legge e delle ulteriori disposizioni impartite durante le operazioni di trattamento dei dati da parte dei Delegati e Responsabili, Amministratori di Sistema e Autorizzati al trattamento.
I controlli e le verifiche sono effettuati previa programmazione periodica o in caso di necessità anche su sollecitazione degli interessati e le relative attività sono svolte dal personale a ciò autorizzato sotto il coordinamento dell'Ufficio di Staff, di concerto con il DPO.

ARTICOLO 31
LA FORMAZIONE DEI DELEGATI, AUTORIZZATI E AMMINISTRATORI DI SISTEMA

Il Titolare inserisce nel proprio Piano Annuale di Formazione iniziative atte ad assicurare la formazione e il continuo aggiornamento dei Delegati al trattamento, degli Autorizzati da questi coordinati, degli Amministratori di Sistema e, in generale, di tutto il personale sui temi della protezione dei dati personali e sui diritti, doveri ed adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali.
I Responsabili del trattamento sono tenuti ad assicurare al Titolare che gli Autorizzati e gli Amministratori di Sistema, che svolgono attività di trattamento di dati personali su loro mandato, siano formati e continuamente aggiornati; di tale formazione dovrà essere data evidenza, su richiesta, al Titolare del trattamento.

ARTICOLO 32
LA DISCIPLINA DELLE MISURE DEL REGOLAMENTO

Nelle forme e con le modalità previste dal proprio sistema di gestione, il Titolare provvede ad adottare procedure, disciplinari, linee guida, indicazioni operative e regolamenti di settore che consentano l'applicazione del presente Regolamento e delle misure di legge a protezione dei dati personali.
Il Titolare persegue, per la protezione dei dati personali, il continuo miglioramento qualitativo, attraverso l'emanazione di specifici provvedimenti e procedure, linee guida operative e comportamentali.

ARTICOLO 33
NORME TRANSITORIE E FINALI

Per tutto quanto non espressamente previsto dal presente Disciplinare, si applica la normativa vigente in tema di protezione dei dati personali e amministrazione digitale.
Il Titolare si riserva di adeguare, modificare o integrare il testo del presente Disciplinare per motivi organizzativi e/o in caso di eventuali modifiche normative.
13/06/2019
Canicattì
Data e luogo di redazione.