ENTE DI GESTIONE DELLE AREE PROTETTE DELLA VALLE SESIA
PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO
A TUTELA DEI DATI PERSONALI

Sommario

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento generale in materia di Protezione dei Dati personali. Il GDPR, acronimo di "*General Data Protection Regulation*" va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo. Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea. Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

Il nuovo apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di accountability (nell'accezione inglese).

Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal GDPR, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati dal regolamento.

Come specifica chiaramente l'art. 25 del GDPR, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*" ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal GDPR, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.

Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "Modello organizzativo e di gestione" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa dell'Ente, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un Modello ad hoc è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.

L'adeguamento al Regolamento UE 2016/679 impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, l'approvando Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente modello organizzativo contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno dell'Ente, nelle sue articolazioni gerarchiche.

E' ammesso ed anzi incoraggiato l'utilizzo di modulistica differente rispetto a quella allegata al presente modello a condizione che essa ne rispetti i criteri e le regole generali.

Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

PARTE I - NORME E PRINCIPI GENERALI

Questo Ente assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza. In attuazione del suddetto principio l'Ente assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei seguenti principi:

a) «*liceità, correttezza e trasparenza*»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) «*limitazione delle finalità*»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, paragrafo 1 del RGDP, considerato incompatibile con le finalità iniziali;

c) «*minimizzazione dei dati*»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «*necessità*»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;

e) «*esattezza*»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

f) «*limitazione della conservazione*»: i dati personali 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;

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

h) «*responsabilizzazione*»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

SENSIBILIZZAZIONE E FORMAZIONE

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l'Ente sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, questo Ente riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con l'Ente.

Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie.

L'Ente organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Ente.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

TRATTAMENTO DEI DATI PERSONALI

L'Ente tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto infra nel presente documento. Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Al fine di garantire la correttezza delle operazioni di trattamento l'Ente provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al GDPR.

Tipologie di dati trattati

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali l'Ente, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del GDPR;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'articolo 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del GDPR (c.d. dati giudiziari)

Finalità del trattamento

L'Ente effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche sensibili (e super-sensibili) e giudiziari.

L'Ente rende disponibile attraverso il proprio sito web istituzionale una pagina contenente le informazioni sul trattamento dei dati personali ad opera dei propri uffici e servizi, conformemente a quanto previsto dagli articoli 13 e 14 del GDPR.

CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, l'Ente favorisce la circolazione all'interno dei propri uffici dei dati personali degli interessati il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR.

La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti.

Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

COORDINAMENTO DI NORME

Questo Ente intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato ad opera dei cittadini, nelle varie forme in cui il diritto di accesso è riconosciuto, quali (a titolo esemplificativo) quella prevista dal TUEL (D.Lgs. 267/2000) negli articoli 10 e 43, quella prevista dalla Legge 241/90 e quella prevista dal D.Lgs. 33/2013.

A tale proposito - fermo restando che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore – gli Uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'Ufficio, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

PARTE II - PROFILO ORGANIZZATIVO

PROFILO STRUTTURALE
La prima risposta organizzativa è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa dell'Ente, integrandosi con essa. La creazione di tale struttura comporta tre azioni principali:
• il disegno di struttura (organigramma) per la Privacy;
• la definizione dei ruoli;
• l'individuazione dei soggetti "abilitati" dall'Ente a trattare i dati personali.
Conseguente, alla costruzione, sarà quindi necessario adeguare le competenze mediante la formazione e informazione dei soggetti, abilitando concretamente i soggetti stessi.

IL TITOLARE DEL TRATTAMENTO

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto all'Ente locale) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*".

Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:
a) determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
b) mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);
c) garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
d) individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
f) designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
g) istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
h) effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
i) comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
l) ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
m) rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
o) rispondere delle violazioni amministrative ai sensi del GDPR (art. 83)

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che titolare del trattamento sia l'Ente nel suo complesso in quanto la legislazione nazionale e regionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Tuttavia, in concreto, esso manifesta la propria volontà attraverso

coloro a cui è attribuito il potere di decidere per l'Ente, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.

Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi dell'Ente in relazione alle funzioni agli stessi assegnati dal D.Lgs. n. 267/2000 e dallo statuto. Tale ripartizione è così intesa da questa Amministrazione:

A. alla **Comunità delle Aree protette**, sono assegnate competenze di tipo consultivo e propositivo con specifico riferimento alle tematiche ambientali;
B. all'organo esecutivo (**Consiglio**) sono assegnate tutte le competenze a carattere non gestionale, con particolare riferimento agli atti ed attività a contenuto programmatico, organizzativo e di indirizzo dell'attività complessiva dell'Ente. Allo stesso competono l'adozione del modello organizzativo e le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Direttore;
C. all'organo di vertice (**Presidente**) compete la designazione del Responsabile della protezione dei dati. Il Presidente sta inoltre in giudizio nei procedimenti giurisdizionali di qualsiasi natura e tipo (civili, amministrativi e penali) e promuove le azioni e i provvedimenti più opportuni e necessari per la tutela degli interessi del Parco;
D. al **Direttore** competono le funzioni di tipo manageriale, organizzativo, di designazione e di coordinamento dei Responsabili di posizione organizzativa. Spetta inoltre di:
a) adottare soluzioni di privacy by design e by default;
b) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
c) disporre l'adozione dei provvedimenti imposti dal Garante;
d) la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
e) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
f) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
g) individuare i responsabili (esterni) ed i contitolari del trattamento fornendo le necessarie indicazioni.
h) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
E. ai **Responsabili di posizione organizzativa**, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) contribuire al costante aggiornamento del registro delle attività di trattamento;
d) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
e) garantire al Responsabile della protezione dei dati personali ed al personale (eventualmente) designato Amministratore di sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

IL DESIGNATO (O AUTORIZZATO) AL TRATTAMENTO

Il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

Il Codice privacy, all'articolo 2-quaterdecies prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Il GDPR e la normativa nazionale di adeguamento consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne all'Ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, ma non anche ai sensi del GDPR, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo ed a qualunque livello) all'interno dell'Ente è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.

Gli specifici compiti e funzioni attribuiti al designato e connessi al trattamento dei dati personali sono elencati nel documento Allegato sub 1).

RESPONSABILE DI POSIZIONE ORGANIZZATIVA - DESIGNATO AL TRATTAMENTO

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed il Responsabile del trattamento possono designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Questa Amministrazione ritiene dunque che il Responsabile di P.O. debba essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al paragrafo che precede.

Considerato che al Responsabile di P.O. spettano l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'Ente verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo e che egli è responsabile, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui è preposto, appare opportuno attribuirgli specifici compiti e funzioni spettanti al Titolare, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo.

Ferma restando l'elencazione degli specifici compiti e funzioni attribuiti al Responsabile di P.O. ai sensi dell'Allegato sub 1), ad esso sono altresì assegnati quelli di cui all'Allegato sub 2).

DIRETTORE - DESIGNATO AL TRATTAMENTO

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed il Responsabile del trattamento possono designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Questa Amministrazione ritiene dunque che il Direttore debba conseguentemente essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità ai paragrafi che precedono.

Ferma restando l'elencazione degli specifici compiti e funzioni attribuite al Direttore ai sensi dell'Allegato sub 1), al medesimo sono altresì assegnati quelli di cui all'Allegato sub 3).

IL CONTITOLARE DEL TRATTAMENTO

In base alla previsione contenuta nell'articolo 26 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*".

In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.

Spetta al Direttore identificare gli eventuali contitolari di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni per il trattamento dei dati - sulla base delle indicazioni contenute nell'Allegato sub 4) al presente modello organizzativo - avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai contitolari l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.

Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. E' tuttavia ammessa una diversa ripartizione "Interna" del profilo di responsabilità, da valutarsi caso per caso.

Il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione degli interessati nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

IL RESPONSABILE DEL TRATTAMENTO

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal Titolare ed elaborare i dati personali per conto di quest'ultimo.

La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare.

Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Ente ed un altro soggetto, pubblico o privato possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo Ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169).

Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Spetta al Direttore identificare i responsabili e gli eventuali sub responsabili di riferimento della struttura organizzativa di competenza e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati - sulla base delle indicazioni contenute nell'Allegato sub 5) al presente modello organizzativo - avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.

Direttore ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni.

La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

L'Ente si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD o DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

I dati identificativi e di contatto del Responsabile della protezione dei dati sono pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link, comunicati all'Autorità di controllo, comunicati ai componenti degli organi di governo, a tutti i dipendenti dell'Ente, ai componenti degli organi di controllo interni nonché sono inclusi in tutte le informative rese agli interessati ai sensi degli articoli 14 e 14 del GDPR.

PARTE III - ADEMPIMENTI E PROCEDURE

MISURE PER LA SICUREZZA DEI DATI PERSONALI

Il Consiglio Direttivo, il Direttore ed i Responsabili di P.O. provvedono, per quanto di competenza, all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi con cui sono trattati i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Ai sensi dell'articolo 30 del GDPR "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*"; la medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.

Un'altra grande differenza rispetto al D.lgs. 196/2003 è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.

E' intenzione dell'Ente adottare un sistema informatico che meglio possa consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico dovrà rispettare il contenuto prescritto dal GDPR e dovrà tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.

In ragione delle dimensioni, anche organizzative di questa Amministrazione, le operazioni tecniche connesse all'istituzione, alla compilazione ed all'aggiornamento delle informazioni contenute nel Registro sono demandate ad un fornitore di servizi software esterno, scelto nel rispetto della vigente normativa in materia di appalti pubblici, il quale presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Tale soggetto esterno sarà designato quale Responsabile del trattamento.

Spetta al Direttore ed al Responsabile di P.O.:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, al fine di consentire la compilazione del registro;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;

- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare;
- contribuire alla tenuta del registro in relazione ai trattamenti della struttura organizzativa di competenza, fornendo le necessarie informazioni e valutazioni

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del DPO.

Ai sensi dell'art. 39 del GDPR che disciplina infatti le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre è tenuto a "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*".

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normativa.

VALUTAZIONI DI IMPATTO SULLA PROTEZIONE DEI DATI

Nel caso in cui una tipologia di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile di P.O., prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità.

Il Direttore conduce quindi una prima fase di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento sia conforme al GDPR e, in seconda battura, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA. L'attività quindi si compone di 3 sottofasi:

a. descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, …) sulla scorta delle risultanze contenute nell'apposito registro;

b. valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del GDPR; rispetto dei diritti degli interessati di cui al capo III del GDPR);

c. valutazione della obbligatorietà di condurre una DPIA;

Fermo restando quanto indicato dall'art. 35, paragrafo 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Direttore, sentito il Responsabile della protezione dei dati, ritenga motivatamente che non possa presentare un rischio elevato; il Direttore può, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;

b) se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal Responsabile della protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni

dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

Una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. L'attività si compone in ulteriori 4 sotto-fasi:

a. raccolta delle informazioni per l'analisi dei rischi (informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.). Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato)

b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromette un asset (informativo) (alcuni esempi sono gli impatti derivanti da una violazione della sicurezza fisica; da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio, perdite dovute a frodi; turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio, perdite di autonomia);

c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;

d. piano di trattamento dei rischi;

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

1) delle finalità specifiche, esplicite e legittime;
2) della liceità del trattamento;
3) dei dati adeguati, pertinenti e limitati a quanto necessario;
4) del periodo limitato di conservazione;
5) delle informazioni fornite agli interessati;
6) del diritto di accesso e portabilità dei dati;
7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;

e) l'acquisizione del parere del Responsabile della protezione dei dati personali

Assume quindi fondamentale importanza l'attività di formalizzazione dei risultati la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

L'Ufficio può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Direttore garantisce l'effettuazione della DPIA ed è responsabile della stessa, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno all'Ente.

Il Direttore deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Direttore devono essere documentate nell'ambito della DPIA.

L'Ufficio deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il GDPR, in particolare qualora l'Ufficio non abbia identificato o attenuato sufficientemente il rischio). L'Ufficio consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti ed un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al GDPR, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione dell'Ente, presenza di nuove minacce, ecc.).

Il Responsabile della protezione dei dati personali monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Eventuali Responsabili del trattamento collaborano e assistono l'Ufficio oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Dal punto di vista operativo - considerata la complessità di un processo DPIA e relativa fase di analisi dei rischi – l'Ufficio deve adottare strumenti applicativi specializzati in grado di gestire tutte le fasi del processo ed in grado di riproporre la sua applicabilità nel tempo.

E’ pubblicata sul sito istituzionale dell’Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all’effettuazione della DPIA.

VIOLAZIONE DEI DATI PERSONALI

Il Titolare predispone una idonea procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l’Ente (**data breach policy**).

I dati oggetto di riferimento saranno i dati personali trattati “da “e “per conto” del Titolare, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

L’obiettivo del presente documento sarà, pertanto:

• sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all’importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);

• definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;

• definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;

• assicurare un adeguato flusso comunicativo all’interno della struttura del Titolare tra le parti interessate.

PARTE IV - DIRITTI DELL'INTERESSATO

INFORMATIVA, COMUNICAZIONE E MODALITÀ TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

L'Ente adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal GDPR in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni di cui agli articoli 13 e 14 del GDPR sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale e mediante pubblicazione del relativo testo nella sezione Amministrazione trasparente del portale (Informativa estesa). Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Ente è predisposta apposita informativa.

Una informativa breve è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture dell'Ente, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con l'Ente;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc..

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'Ente agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18 del GDPR. Nei casi di cui all'articolo 11, paragrafo 2, del GDPR l'Ente non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che dimostri di non essere in grado di identificare l'interessato.

L'Ente fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal GDPR, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'Ente informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta dell'interessato, l'Ente informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal GDPR sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, l'Ente può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta. Incombe all'Ente l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Fatto salvo l'articolo 11 del GDPR, qualora l'Ente nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal GDPR, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

ALLEGATO 1

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AI SOGGETTI DESIGNATI

Il Titolare del trattamento, in forza del principio di «responsabilizzazione», impartisce alla persona fisica designata e delegata al trattamento, le istruzioni a cui è obbligata ad attenersi, sotto la comminatoria delle sanzioni di legge e di contratto.

In particolare, nella gestione dei processi/procedimenti dell'Ufficio a cui la persona fisica designata al trattamento è preposta e, più in generale, nello svolgimento dell'attività lavorativa presso detto Ufficio, la delega ad effettuare le operazioni di trattamento dei dati personali nell'ambito della suddetta attività, e descritte nel documento Registro delle attività di trattamento del Titolare, viene rilasciata con le seguenti istruzioni che costituiscono cogenti prescrizioni, anche ai fini della responsabilità personale e disciplinare:

- in attuazione del principio di «liceità, correttezza e trasparenza»,
    - le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;
    - autorizzazione a comunicare od eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui la persona fisica designata e delegata al trattamento è preposta;
- in attuazione del principio di «limitazione della finalità» il trattamento dev'essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione»
    - evitare di creare banche dati nuove senza espressa autorizzazione del Direttore o del Responsabile di P.O.;
    - conservare i dati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nell'Ufficio di competenza, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del GDPR vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato, fatte salve le norme in materia di archiviazione amministrativa;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare:
    - riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;

- non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per fax, documenti in chiaro contenenti dati personali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice). In alternativa, si suggerisce di avvisare preventivamente il destinatario della comunicazione fax in modo che possa curarne la diretta ricezione;

- In attuazione del principio di «trasparenza»:
  - accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
  - fornire all'Interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del GDPR, relative al trattamento utilizzando la modulistica all'uopo predisposta dal Titolare. Se richiesto dall'Interessato, le informazioni medesime possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato;
  - ove si renda necessario, segnalare al Direttore o Responsabile di P.O. la necessità di adeguamento, correzione ed integrazione della modulistica in uso all'Ufficio;
  - conservare, nel rispetto del principio di accountability, tutte le versioni delle informative in uno specifico archivio interno cartaceo e telematico e di tenere traccia di tutte le modifiche al testo (connesse alle modifiche organizzative, tecniche e normative) al fine di consentire al Titolare una maggiore tutela in sede amministrativa e/o giudiziaria nel caso di reclami o procedimenti giudiziari per risarcimento di danni conseguenti a trattamenti illeciti di dati;
  - agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR. In particolare, qualora riceva richieste provenienti dagli interessati, finalizzate all'esercizio dei propri diritti, dovrà:
    - darne tempestiva comunicazione al Direttore o Responsabile di P.O., allegando copia delle richieste ricevute;
    - coordinarsi, ove necessario e per quanto di propria competenza, con il Direttore o Responsabile di P.O. per gestire le relazioni con gli Interessati;

- seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del GDPR ed a sostenere i relativi test finali finalizzati alla verifica dell'apprendimento;
- segnalare al Direttore o Responsabile di P.O., con tempestività, eventuali anomalie, incidenti, furti, perdite accidentali di dati connessi con una ricaduta sul trattamento dei dati personali, al fine di attivare le procedure di comunicazione delle violazioni di dati all'Autorità di controllo ed ai soggetti autorizzati (istituto del c.d. data breach o violazione di dati personali);
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a propria disposizione ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
- assistere il Titolare del trattamento nella tenuta del registro delle attività di trattamento istituito ai sensi dell'articolo 30 del GDPR, tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
- segnalare al Direttore o Responsabile di P.O., con tempestività, eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Direttore o Responsabile di P.O. e secondo le modalità stabilite dal medesimo;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

- fornire al Direttore o Responsabile di P.O., a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare del trattamento, nel suo complesso ed articolazioni, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- nel caso di presenza di utenti, ospiti o personale di servizio, all'interno dell'Ufficio, sarà necessario:
    - che la persona non sia visibile dall'esterno;
    - non ammettere in ufficio altre persone se non espressamente richiesto e in accordo con l'utente con cui stiamo parlando;
    - apporre fuori dalla porta una targhetta o altro equivalente che indichi che è in corso un colloquio;
    - fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
    - evitare che l'utente esponga le proprie questioni personali prima di accedere all'ufficio (se necessario, spiegare alla persona la motivazione);
    - è importante che sulla scrivania vi siano solo informazioni neutre ed impersonali e, comunque, appartenenti alle categorie di cui agli articoli 9 e 10 del GDPR;
    - evitare di allontanarsi dalla scrivania o riporre i documenti ed attivare il salvaschermo del PC;
    - durante il colloquio non devono essere ricevute telefonate; se necessario, rispondere e rinviare a più tardi la conversazione telefonica. Se nell'ufficio è inserita una segreteria telefonica assicurarsi sempre che, in presenza di persone, il volume sia al minimo e che i messaggi eventualmente lasciati non possano essere sentiti;
    - assicurarsi che schedari e armadi che contengono dati personali siano chiusi a chiave quando siamo assenti dall'ufficio, salvo che sia possibile chiudere l'ufficio stesso;
    - bloccare l'accesso ad estranei dell'ufficio.

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.
In particolare, per tali trattamenti la persona fisica designata e delegata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) Strumenti elettronici in generale

1) i personal computer fissi e portatili ed i programmi per elaboratore su di essi installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Titolare e nel rispetto delle indicazioni da questo fornite;

2) in generale tutti i dispositivi elettronici sono forniti al dipendente per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali;

3) le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione stessa. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte del Direttore o Responsabile di P.O.

4) assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;

5) rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al Direttore o competente Responsabile di P.O.;

6) per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma software;
7) il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen drive e supporti di memoria.

B) **Password e username (credenziali di autenticazione informatica)**

1) per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti. Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise con altri incaricati del trattamento;
2) è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
3) i codici identificativi, le password e le smart card dei dipendenti saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituire la propria smart card agli uffici a ciò preposti. 4) la password che la persona fisica designata e delegata al trattamento imposta, con il supposto e l'assistenza, in caso di difficoltà, del Direttore o Responsabile di P.O.:

- deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri;
- non deve essere riconducibile alla persona del designato;
- deve essere cambiata almeno ogni 3 mesi dal designato medesimo;
- non dev'essere rivelata o fatta digitare al personale di assistenza tecnica;
- non dev'essere rivelata o comunicata al telefono, via fax od altra modalità elettronica. Nessuno è autorizzato a chiederla;

C) Assenza od impossibilità temporanea o protratta nel tempo

1) nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell'area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.
2) in caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Direttore o Responsabile di P.O. può richiedere con apposita e motivata richiesta rivolta a personale od aziende competenti di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Direttore o Responsabile di P.O. deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

D) Log-out

In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il

dipendente deve attivare il salvaschermo con password o deve bloccare il computer (utilizzando i tasti CTRL+ALT+CANC) e togliere la smart card dall'apposito alloggiamento.

E) **Utilizzo della rete internet e relativi servizi - Cloud storage**

1) non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;
2) è da evitare la registrazione a servizi online, a titolo o di interesse personale;
3) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Direttore o Responsabile di P.O. e con il rispetto delle normali procedure di acquisto;
4) non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
5) la persona fisica designata e delegata al trattamento, si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

F) Posta elettronica

1) la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;
2) si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati dal Titolare per le comunicazioni personali;
3) al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'Ente, eventualmente affiancandoli a quelli individuali;
3) le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
4) non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
5) la posta elettronica diretta all'esterno della rete dell'Ente può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR;
6) non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale dell'Ente per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;
7) qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente il Direttore o Responsabile di P.O..

G) **Software, applicazioni e servizi esterni**

1) onde evitare pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Direttore o Responsabile di P.O.
2) non è consentito uti1izzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
3) non è consentito modificare le configurazioni impostate sul proprio PC;
4) non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di account privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale;
6) il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti

istruzioni;
7) tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dai dipendenti, (salvo quando questo sia richiesto per compiere attività di manutenzione o aggiornamento).

H) **Reti di comunicazione**

1) nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC;
2) nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre a servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore;
3) le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
4) al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, il dipendente dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;
5) è proibito tentare di acquisire i privilegi di amministratore di sistema;
6) non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.
7) non condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine condividere materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

I) Supporti esterni di memorizzazione

La persona fisica designata e delegata al trattamento, ha l'obbligo di:

- utilizzare i supporti di memorizzazione solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati contemplati dagli articoli 9 e 10 del GDPR devono essere espressamente autorizzate dal Direttore o Responsabile di P.O. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del Direttore o del Responsabile di P.O.
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati;

ALLEGATO 2

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AL RESPONSABILE DI P.O.

Ferma restando la necessaria osservanza dei compiti e funzioni di cui al precedente Allegato 1, spetta al Responsabile di P.O.:

SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

- collaborare con il Direttore e gli altri Responsabili di P.O. per l'elaborazione degli obiettivi strategici ed operativi del sistema di sicurezza e di protezione dei dati personali da sottoporre all'approvazione del Titolare;
- collaborare con il Direttore e gli altri Responsabili di P.O. per l'elaborazione della pianificazione strategica del sistema di sicurezza e di protezione dei dati personali attraverso l'elaborazione di un Piano per la sicurezza/protezione, da sottoporre all'approvazione del Titolare;
- collaborare con il Direttore e gli altri Responsabili di P.O. per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di c.d. data breach, da sottoporre all'approvazione del Titolare;
- collaborare con il Titolare del trattamento per l'inserimento degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali nel Piano della Performance/PDO nonché nel DUP e negli altri strumenti di pianificazione del Titolare;
- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ente, da sottoporre all'approvazione del Titolare;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa, con obbligo di sottoporre l'aggiornamento all'approvazione del Titolare;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare;
- mettere in atto le misure tecniche ed organizzative adeguate, identificate dal Titolare, funzionali a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
  a) la pseudonimizzazione e la cifratura dei dati personali;
  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- mettere in atto le misure tecniche ed organizzative adeguate, identificate dal Titolare per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
  a) tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
  b) dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica
- proporre e suggerire al Titolare misure tecniche ed organizzative ritenute necessarie a garantire la protezione dei dati dal trattamento, in relazione ai trattamenti della struttura organizzativa di competenza;

- contribuire alla tenuta del registro delle attività di trattamento in relazione ai trattamenti della struttura organizzativa di competenza;
- cooperare, su richiesta, con il RPD/DPO e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
- in caso di violazione dei dati personali, collaborare con il Titolare, il RPD/DPO nel processo di notifica della violazione all'Autorità di controllo competente senza ingiustificato ritardo e, comunque, entro 24 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 delle persone fisiche;
- assicurarsi che il RPD/DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD/DPO nell'esecuzione dei compiti assegnati, fornendogli le risorse necessarie per assolvere tali compiti, per accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica;
- documentare e tracciare, per iscritto, ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;
- collaborare con il Titolare per inserimento dei rischi di corruzione, illegalità e degli illeciti in materia di trattamento di dati personali negli aggiornamenti annuali al PTPC e collaborare al RPC per le segnalazioni degli illeciti relativi al trattamento dei dati;
- documentare tutte le attività e gli adempimenti delegati e, in ogni caso, tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;
- controllare e monitorare la conformità dell'analisi, della valutazione dei rischi e della valutazione di impatto nonché controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;
- tracciare documentalmente le attività di controllo e monitoraggio mediante periodici report/resoconti/referti da sottoporre al Titolare ed al RPD/DPO;
- conformare il trattamento ai pareri ed indicazioni del RPD/DPO e dell'Autorità di controllo nonché alle linee guida ed ai provvedimenti dell'Autorità di controllo;
- formulare proposte, in occasione dell'approvazione/aggiornamento annuale degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;
- attuare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto;
- promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
- effettuare ogni ulteriore attività, anche se non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa di riferimento.

ALLEGATO 3

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AL DIRETTORE

Ferma restando la necessaria osservanza dei compiti e funzioni di cui al precedente Allegato 1, spetta al Direttore di osservare le prescrizioni che seguono.

SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

- collaborare con i Responsabili di P.O. per l'elaborazione degli obiettivi strategici ed operativi del sistema di sicurezza e di protezione dei dati personali da sottoporre all'approvazione del Titolare;
- collaborare con i Responsabili di P.O. per l'elaborazione della pianificazione strategica del sistema di sicurezza e di protezione dei dati personali attraverso l'elaborazione di un Piano per la sicurezza/protezione, da sottoporre all'approvazione del Titolare;
- collaborare con i Responsabili di P.O. per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di c.d. data breach, da sottoporre all'approvazione del Titolare;
- collaborare con il Titolare del trattamento per l'inserimento degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali nel Piano della Performance/PDO nonché nel DUP e negli altri strumenti di pianificazione del Titolare;
- proporre e suggerire al Titolare misure tecniche ed organizzative ritenute necessarie a garantire la protezione dei dati dal trattamento, ulteriori rispetto a quelle già in atto;
- cooperare, su richiesta, con il RPD/DPO e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
- assicurarsi che il RPD/DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD/DPO nell'esecuzione dei compiti assegnati;
- conformare il trattamento ai pareri ed indicazioni del RPD/DPO e dell'Autorità di controllo nonché alle linee guida ed ai provvedimenti dell'Autorità di controllo;
- coordinare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa del Titolare;
- identificare contitolari, responsabili e sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni ed i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
- acquisire dai contitolari, responsabili e sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari, responsabili e sub responsabili risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni;
- effettuare, prima di procedere al trattamento, quando questo può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;
- prima di procedere al trattamento, consultare l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
- in caso di violazione dei dati personali, procedere alla notifica della violazione all'Autorità di controllo competente senza ingiustificato ritardo e, comunque, 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 delle persone fisiche;

- in caso di violazione dei dati personali, comunicare la violazione all'Interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- formulare proposte, in occasione dell'approvazione/aggiornamento annuale degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;
- attuare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto;
- identificare e designare, per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del Titolare ed attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni e controllando costantemente che le persone fisiche designate, delegate e autorizzate al trattamento dei dati effettuino le operazioni di trattamento:
  - in attuazione del principio di «liceità, correttezza e trasparenza»;
  - in attuazione del principio di «minimizzazione dei dati»;
  - in attuazione del principio di «limitazione della finalità»;
  - in attuazione del principio di «esattezza»;
  - in attuazione del principio di «limitazione della conservazione»;
  - in attuazione del principio di «integrità e riservatezza»;
  - in attuazione del principio di «liceità, correttezza e trasparenza».
- promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
- effettuare ogni ulteriore attività, anche se non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa di riferimento.

ALLEGATO 4

BOZZA DI ACCORDO DI CONTITOLARITA'

AI SENSI DELL'ART. 26 DEL REGOLAMENTO (EU) 2016/679

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, entrambe le parti saranno identificate, congiuntamente, quali "Contitolari" o "Parti")

PREMESSO CHE

1) è in essere tra le Parti un progetto comune consistente in _____, il quale comporta la necessità di determinare congiuntamente le finalità e le modalità del trattamento dei dati personali coinvolti nella realizzazione del medesimo progetto comune;

2) che in data 25 maggio 2018 è divenuto pienamente operativo il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora innanzi, più semplicemente, "GDPR");

3) l'articolo 4, paragrafo 1, n. 7) del GDPR definisce quale 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*";

4) a norma dell'articolo 26, paragrafo 1 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*";

5) a norma dell'articolo 26, paragrafo 2 del GDPR "*L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato"*;

6) è intenzione delle Parti contraenti regolamentare in modo trasparente i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché i rispettivi ruoli nella comunicazione delle informazioni agli interessati, addivenendo alla sottoscrizione della presente accordo;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, i Contitolari dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni di legge vigenti e nel pieno rispetto delle linee guida e dei codici di condotta applicabili, di volta in volta approvati dall'Autorità di controllo.

2. Resta inteso tra le Parti che, ai sensi dell'art. 26, comma 3, del Regolamento (EU) 2016/679, indipendentemente dalle disposizioni del presente Accordo, l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Contitolare del trattamento.
3. In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.
4. Il presente accordo non determina l'insorgere di alcun diritto alla revisione di prezzi od altre forme di impegno, anche economico, già definiti tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
5. Il presente accordo annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla sua stipulazione, i loro rapporti saranno regolati esclusivamente dal presente accordo.
6. Qualsiasi modifica od integrazione del presente accordo potrà farsi soltanto per iscritto a pena di nullità.
7. Il contenuto essenziale di questo accordo di Contitolarità è messo a disposizione dell'Interessato nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

Articolo 2 - Oggetto del trattamento
1. I Contitolari dichiarano, in merito al trattamento dei Dati Personali, di condividere le decisioni relative alle finalità e modalità del trattamento di dati e, in particolare:
- le seguenti banche dati; dipendenti e collaboratori, _____;
- le finalità del trattamento di dati personali, ciascuna con le proprie specificità legate alle attività concretamente svolte;
- i mezzi del trattamento e le modalità del trattamento di dati personali;
- la politica di conservazione dei dati;
- lo stile e le modalità di comunicazione delle informative art. 13 del GDPR;
- la procedura di gestione dei consensi (ove necessari);
- la designazione e la formazione dei soggetti autorizzati;
- istruzioni sull'uso degli strumenti informatici per il personale;
- la gestione delle comunicazioni e nomine dei responsabili ai sensi dell'art. 28 del GDPR;
- la tenuta dei registri del trattamento ai sensi dell'art. 30 del GDPR;
- le procedure nel caso di trasferimento dei dati fuori UE;
- gli strumenti ed i mezzi utilizzati per l'attuazione delle decisioni e in parte anche per l'operatività dei Contitolari soprattutto in relazione alle misure di sicurezza fisiche, organizzative e tecniche;
- l'approccio basato sul rischio;
- i profili e la politica di sicurezza dei dati personali, la procedura del Data Breach e la procedura di valutazione di impatto sulla protezione dei dati personali (DPIA);
- la gestione della procedura di esercizio dei diritti dell'Interessato;
- una raccolta congiunta delle procedure sulla protezione dei dati personali attraverso la tenuta comune e gestione di un modello organizzativo.
2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati già presenti, in tutti gli archivi sia cartacei che informatizzati, e di tutti quelli che si acquisiranno in futuro. Il flusso dei dati personali sarà così strutturato: _____.
3. Con il presente accordo i Contitolari convengono che i dati personali presenti negli archivi tanto cartacei quanto informatizzati, nonché quelli futuri, verranno trattati per le seguenti finalità: _____.
4. Le attività alla base del presente accordo comportano il trattamento delle seguenti categorie di dati personali: _____.
5. Le categorie di Interessati sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Il presente accordo diviene efficace tra le parti immediatamente all'atto della sua sottoscrizione e sarà valido ed efficace sino alla scadenza, originale o prorogata del rapporto convenzionale che lega i Contitolari, ovvero alla sua cessazione di validità ed efficacia a qualsiasi causa dovuta.
2. Il Trattamento dei dati personali in regime di contitolarità, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati dei Contitolari in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello in precedenza indicato, fatto salvo che il trattamento e la conservazione dei dati medesimi ad opera di ciascuno dei Contitolari sia imposta dalla normativa vigente.
3. A seguito della cessazione del trattamento, nonché a seguito della cessazione del rapporto convenzionale sottostante, qualunque ne sia la causa, i Contitolari saranno tenuti a provvedere alla integrale distruzione dei dati personali trattati, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità od il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte dei singoli Contitolari, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
4. Ciascun Contitolare provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate nell'ambito del progetto comune. Sul contenuto di tale dichiarazione l'altro Contitolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

Articolo 4 – Obblighi tra le parti
1. La tutela dei dati personali è fondata sull'osservanza dei principi illustrati nel presente documento che i Contitolari si impegnano a diffondere, rispettare e far rispettare ai propri amministratori, ai propri dipendenti e collaboratori ed ai soggetti terzi con cui collaborano nello svolgimento della propria attività istituzionale. In particolare i Contitolari sono impegnati affinché la politica della protezione dati personali, e quanto ne consegue, sia compresa, attuata e sostenuta da tutti i soggetti, interni ed esterni, coinvolti nelle attività dei Contitolari, tenuto conto della loro realtà concreta, delle loro possibilità anche economiche e dei loro valori.
2. I Contitolari si impegnano a mantenere e garantire la riservatezza e la protezione dei dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità. In particolare essi, anche disgiuntamente tra loro, si impegnano a:
a) comunicare e diffondere la propria politica in merito alla protezione dei dati personali;
b) prestare ascolto e attenzione a tutte le parti interessate proprie – a mero titolo esemplificativo, amministratori, personale dipendente e collaboratore, cittadini, utenti e beneficiari di prestazioni anche di natura assistenziale, fornitori, consulenti – e tenendo in debito conto le loro istanze in materia di trattamento di dati personali e dando pronto riscontro;
c) trattare i dati personali in modo lecito, corretto e trasparente in linea con i principi costituzionali e con la normativa vigente in materia, in particolare il GDPR, e solo per il tempo strettamente necessario alle finalità previste, comprese quelle per ottemperare agli obblighi di legge;
d) raccogliere i dati personali limitandosi a quelli indispensabili per effettuare le attività costituenti il progetto comune (dati personali pertinenti e limitati);
e) trattare i dati personali secondo i principi di trasparenza per le sole finalità specifiche ed espresse nelle proprie informative;
f) adottare processi di aggiornamento e di rettifica dei dati personali trattati per assicurarsi che i dati personali siano, per quanto possibile, corretti e aggiornati;
g) conservare e tutelare i dati personali di cui è in possesso con le migliori tecniche di preservazione disponibili;
h) garantire il continuo aggiornamento delle misure di protezione dei dati personali. Tale impegno sarà costantemente seguito nell'ambito del principio di responsabilizzazione mettendo in atto, con costanza, misure tecniche e organizzative adeguate e politiche idonee, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR tenuto conto dello stato dell'arte, della natura dei dati personali custoditi e dei rischi ai quali sono esposti. Ciascun Contitolare eseguirà un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;
i) garantire il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico

l) rendere chiare, trasparenti e pertinenti le modalità di trattamento dei dati personali e la loro conservazione in maniera da garantirne un'adeguata sicurezza;
m) favorire lo sviluppo del senso di responsabilizzazione e la consapevolezza dell'intera organizzazione verso i dati personali, visti come dati di proprietà dei singoli interessati;
n) assicurare il rispetto delle disposizioni legislative e regolamentari applicabili alla tutela dei dati personali aggiornando eventualmente la gestione della protezione dei dati personali;
o) prevenire e minimizzare, compatibilmente con le risorse disponibili, l'impatto di potenziali violazioni o trattamenti illeciti e/o dannosi dei dati personali;
p) promuovere l'inserimento della protezione dati personali nel piano di miglioramento continuo che il Contitolare persegue con i propri sistemi di gestione.
3. I Contitolari si impegnano con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, ad uniformare le modalità, lo stile i modelli e soprattutto le procedure per la protezione dei dati personali a favore dell'Interessato.
4. La comunicazione dei dati personali necessari a garantire il perseguimento del progetto comune avverrà curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati.

Articolo 5 - Incaricati e persone autorizzate
1. Ciascuno dei Contitolari dovrà identificare e designare le persone autorizzate ad effettuare operazioni di trattamento sui dati trattati nel perseguimento del progetto comune, identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e provvedendo alla relativa formazione, anche in merito ai principi di liceità e correttezza a cui deve conformarsi la presente politica per la protezione dei dati personali e il trattamento dei dati personali nonché al rispetto delle misure di salvaguardia adottate.
2. Ciascuno dei Contitolari garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.
3. Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

Articolo 6 - Responsabili del trattamento
1. Ciascuno dei Contitolari il quale ravvisasse la necessità di avvalersi di un responsabile del trattamento per l'esecuzione di specifiche attività richieste nell'ambito del progetto comune, è tenuto a comunicarlo all'altra parte con congruo preavviso.
2. Su tale responsabile del trattamento sono imposti, mediante un contratto od un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, specifici obblighi in materia di protezione dei dati, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge vigente.
3. I rapporti tra i Contitolari e gli eventuali responsabili del trattamento restano disciplinati dall'articolo 28 del GDPR.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali
1. Nei casi previsti dall'art. 35 del GDPR, la valutazione d'impatto sulla protezione dei dati personali ed il suo eventuale riesame, così come la consultazione preventiva di cui all'art. 36 del GDPR, sono a carico di _____, il quale informa tempestivamente l'altro Contitolare della relativa necessità e dell'attività compiuta.
2. In eventuali casi di violazione della sicurezza dei dati personali che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del GDPR è affidata a _____ il quale curerà la predisposizione di un apposito documento (data breach policy), ove non già esistente ed adottato.
3. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:

a) ad informare l'altro Contitolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione fornendogli tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Esso si inoltre attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
4. Ciascun Contitolare si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 8 - Decisioni in merito ai trasferimenti internazionali di dati personali
1. Il presente accordo prevede che i dati personali saranno trattati all'interno del territorio dell'Unione Europea.
2. Nell'ipotesi in cui per questioni di natura tecnica e/o operativa si rendesse necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, il trasferimento dei dati personali, limitatamente allo svolgimento di specifiche attività di Trattamento, sarà regolato in conformità a quanto previsto dal capo V del GDPR. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: (i) su decisioni di adeguatezza dei paesi terzi destinatari espresse dalla Commissione Europea; (ii) su garanzie adeguate espresse dal soggetto terzo destinatario ai sensi dell'articolo 46 del GDPR; (iii) sull'adozione di norme vincolanti d'impresa.

Articolo 9 - Condivisione della procedura per l'esercizio dei diritti dell'Interessato
1. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.
2. In particolare, qualora il referente unitario riceva richieste provenienti dall'Interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:
- darne tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate da ciascun Contitolare per gestire le relazioni con l'Interessato;
- verificare la sussistenza dei presupposti e consentirne, differirne o rifiutarne l'esercizio, dandone tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata.
3. Il referente unitario fornisce altresì assistenza a ciascuno dei Contitolari nell'ambito dei procedimenti amministrativi e giudiziari instaurati dall'Interessato o dall'Autorità di controllo in conseguenza dell'attività di cui al presente articolo.

Articolo 10 - Verifiche circa il rispetto delle regole di protezione dei dati personali
1. Ciascuno dei Contitolari riconosce all'altro il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali nell'ambito del progetto comune. A tal fine, Ciascuno dei Contitolari ha il diritto di disporre – a propria cura e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi dell'altro.
2. Ciascuno dei Contitolari rende disponibile tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire la conduzione di audit, comprese le ispezioni, e per contribuire a tali verifiche.

3. Ciascuno dei Contitolari deve informare e coinvolgere tempestivamente l'altra parte in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 11 - Responsabilità per violazione delle disposizioni
I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali.

Articolo 12 - Responsabile della Protezione dei dati personali
1. Ciascuno dei Contitolari rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del GDPR, individuando quale soggetto idoneo:
_____
Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.

Articolo 13 – Clausole nulle o inefficaci
Qualora una o più clausole del presente accordo fossero o divenissero contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità dello stesso, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'accordo ove la pura e semplice eliminazione della clausola nulla menomasse gravemente i suoi diritti.

Articolo 14 – Comunicazioni
Qualsiasi comunicazione relativa al presente accordo dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'accordo. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 15 – Disposizioni finali
Per quanto non espressamente indicato nella presente Appendice, i rinviano al GDPR, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.

ALLEGATO 5

BOZZA DI APPENDICE CONTRATTUALE

AI SENSI DELL'ART. 28 DEL REGOLAMENTO (EU) 2016/679

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, più semplicemente, Titolare del trattamento)

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, più semplicemente, Responsabile del trattamento)

PREMESSO CHE

1) tra le parti è in essere un contratto, stipulato in data _____ avente ad oggetto _____ e durata sino a _____ (d'ora innanzi, più semplicemente, Contratto);

2) nel dare esecuzione alle obbligazioni dedotte nel Contratto il Responsabile si troverà ad effettuare operazioni di trattamento di dati personali per conto del Titolare, rimanendo a quest'ultimo di stabilire autonomamente le finalità, le modalità ed i mezzi del trattamento medesimo;

3) che in data 25 maggio 2018 è divenuto pienamente operativo il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora innanzi, più semplicemente, GDPR);

4) l'articolo 4, paragrafo 1, n. 8) del GDPR definisce quale 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*";

5) a norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";

6) a norma dell'articolo 28, paragrafo 3 del GDPR "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*";

7) a norma dell'articolo 28, paragrafo 9 del GDPR "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*"

8) alla data di sottoscrizione della presente appendice non risulta che la Commissione europea ovvero l'Autorità di controllo nazionale abbiano adottato clausole contrattuali tipo ai sensi dei paragrafi 7 ed 8 del GDPR;

9) è intenzione delle Parti contraenti regolamentare i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel GDPR, addivenendo alla sottoscrizione della presente Appendice contrattuale, da considerarsi parte integrante e sostanziale del Contratto;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Il Responsabile è tenuto a trattare i dati personali di cui entra in possesso o rispetto ai quali abbia comunque accesso, in adempimento degli obblighi derivanti dal Contratto e di eventuali servizi accessori allo stesso, nel rispetto dei principi e delle norme contenute nel GDPR ed attenendosi alle istruzioni del Titolare del trattamento, tenendo altresì conto dei provvedimenti, tempo per tempo, emanati dall'Autorità di controllo inerenti al Trattamento svolto.
2. Scopo della presente Appendice è l'identificazione della materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi ed i diritti del Titolare e del Responsabile del trattamento. In particolare, la presente Appendice non costituisce autorizzazione generale ma, bensì, autorizzazione limitata esclusivamente ai trattamenti relativi al servizio specificatamente indicato nel Contratto.
3. La presente Appendice contrattuale non determina l'insorgere di alcun diritto del Responsabile alla revisione del prezzo già definito tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
4. La presente Appendice annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla stipulazione della presente, i loro rapporti saranno regolati esclusivamente dalla presente Appendice.
5. Qualsiasi modifica od integrazione della presente Appendice potrà farsi soltanto per iscritto a pena di nullità.
6. Ciascuna Parte riconosce di essere addivenuta alla stipula della presente Appendice esclusivamente sulla base della rappresentazione dei fatti ricevuta dall'altra Parte e, pertanto, in caso di falsa rappresentazione, la presente Appendice deve intendersi radicalmente nulla sin dall'origine, senza alcuna possibilità di sanatoria, qualsivoglia eccezione intendendosi sin da ora rimossa e/o rinunziata.

Articolo 2 - Oggetto del trattamento

1. Le prestazioni già affidate al Responsabile, ai sensi del Contratto, consistono nell'erogazione dei seguenti servizi: _____.
2. Dette prestazioni comportano il trattamento delle seguenti categorie di dati personali: _____.
3. Le categorie di Interessati sono: _____
4. La natura delle operazioni eseguite sui dati è: _____
5. Le finalità del trattamento dei dati medesimi sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Trattandosi di patto accessorio ed aggiunto al Contratto, esso diviene efficace tra le parti immediatamente all'atto della sua sottoscrizione e sarà valido ed efficace sino alla scadenza, originale o prorogata del Contratto ovvero alla sua cessazione di validità ed efficacia a qualsiasi causa dovuta.
2. Il Trattamento per conto del Titolare, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello in precedenza indicato.
3. A seguito della cessazione del Trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto contrattuale sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto, a discrezione del Titolare, a:
- restituire al Titolare i dati personali trattati, oppure a
- provvedere alla loro integrale distruzione, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) od il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del Trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
4. Il Responsabile, su richiesta del titolare, provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate per conto del Titolare. Sul contenuto di tale dichiarazione il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

5. In caso di fallimento o sottoposizione ad altra procedura concorsuale del Responsabile, ovvero in caso di mancato assolvimento da parte di quest'ultimo degli obblighi previsti ai commi che precedono, ovvero ancora in caso di omissione ovvero di sospensione anche parziale, da parte del Responsabile, dell'esecuzione delle obbligazioni oggetto della presente Appendice, il Titolare, ove possibile e dandone opportuna comunicazione, potrà sostituirsi al Responsabile nell'esecuzione delle obbligazioni ovvero potrà avvalersi di soggetto terzo in danno ed a spese del Responsabile, fatto salvo il risarcimento del maggior danno.

Articolo 4 - Obblighi in capo al Responsabile

1. Il Responsabile dichiara e conferma la propria diretta ed approfondita conoscenza degli obblighi ed oneri derivanti dall'osservanza delle disposizioni contenute nel GDPR, in conseguenza della relazione contrattuale instaurata con il Titolare. Dichiara inoltre di possedere esperienza, capacità e affidabilità idonee a garantire il rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, ed in ogni caso di essere in grado di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa e garantisca la tutela dei diritti dell'Interessato.
2. Il Responsabile prende atto che il Contratto in essere viene mantenuto anche successivamente all'operatività del GDPR per l'esclusiva ragione che il profilo professionale / societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto dal Titolare idoneo a soddisfare i requisiti di esperienza, capacità ed affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti, che possa sollevare incertezze sul loro mantenimento, dovrà essere preventivamente segnalato al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di ritenere risolto il rapporto in essere per fatto e colpa del Responsabile.
3. Il Responsabile è tenuto a:
a) trattare i dati nel rispetto dei principi del trattamento previsti nel GDPR e solo per le finalità indicate dal Contratto. In particolare il Responsabile garantisce che i dati da trattarsi per conto del Titolare, saranno:
a1) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
a2) raccolti per le finalità determinate, esplicite e legittime sopra indicate, e successivamente trattati in modo che non sia incompatibile con tali finalità;
a3) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
a4) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
a5) 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;
b) trattare i dati secondo le istruzioni documentate del Titolare del trattamento dei dati;
c) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate formalmente alla riservatezza od abbiano un adeguato obbligo legale di riservatezza ed abbiano ricevuto la formazione necessaria in materia di protezione dei dati personali;
d) prendere in considerazione, in termini di strumenti, prodotti, applicazioni o servizi, i principi della protezione dei dati in base alla progettazione e per impostazione predefinita (cc.dd. data protection by design e by default);
e) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
4. Il Responsabile si impegna ad informare il Titolare di ogni richiesta, ordine o controllo da parte di una o più Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto della presente Appendice;
5. Il Responsabile informa il Titolare, per quanto di necessità, che i suoi dati verranno conservati e trattati per l'intera durata del rapporto contrattuale e, all'eventuale termine dello stesso, per il tempo previsto dalla vigente normativa, nazionale e comunitaria, in materia contabile, fiscale, civilistica e processuale.

Articolo 5 - Obblighi in capo al Titolare del trattamento

1. Il Titolare del trattamento si impegna a:

a) fornire al Responsabile i dati oggetto del trattamento curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;
b) individuare la base legale del trattamento dei dati personali degli Interessati.
c) documentare, per iscritto, ogni istruzione relativa al trattamento dei dati da parte del Responsabile. Il Responsabile del trattamento informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR od altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
d) assicurare, prima e durante l'intero processo, il rispetto degli obblighi su di sé incombenti ai sensi del GDPR e della normativa nazionale di riferimento;
e) supervisionare il trattamento, in tutte le sue fasi, anche effettuando audit ed ispezioni presso il Responsabile;
f) adottare tutte le misure di sicurezza di sua competenza idonee a garantire il rispetto della normativa in materia di privacy e di trattamento dei dati in regime di sicurezza.
2. Il Titolare si dichiara edotto che in caso di violazione di dati personali (c.d. data breach) rimane a suo carico, ai sensi dell'art. 33 del GDPR, l'obbligo di notifica all'Autorità di controllo senza ingiustificato ritardo e, comunque, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione di dati personali.
3. Il Titolare si impegna, altresì, a comunicare al Responsabile del trattamento qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.
4. Il Titolare rimane responsabile del trattamento dei dati personali attuato tramite procedure applicative sviluppate secondo sue specifiche e/o attraverso propri strumenti informatici o di telecomunicazioni.
5. Il Titolare si impegna ad informare il Responsabile di ogni richiesta, ordine o controllo da parte di una o più Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto della presente Appendice;
6. Il Titolare informa il Responsabile, per quanto di necessità, che i suoi dati verranno conservati e trattati per l'intera durata del rapporto contrattuale e, all'eventuale termine dello stesso, per il tempo previsto dalla vigente normativa, nazionale e comunitaria, in materia contabile, fiscale, civilistica e processuale.

Articolo 6 - Incaricati e persone autorizzate
1. Il Responsabile dovrà identificare e designare le persone autorizzate ad effettuare operazioni di Trattamento sui dati per conto del Titolare identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e provvedendo alla relativa formazione. Allo stesso tempo, il Responsabile dovrà fornire ai soggetti da sé autorizzati le dovute istruzioni relativamente alle operazioni ed alle modalità di trattamento dei dati personali.
2. Il Responsabile garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.

Articolo 7 - Sub-responsabile del trattamento e Terze parti
1. Il Responsabile del trattamento non ricorre ad un altro Responsabile se non previa autorizzazione scritta, del Titolare del trattamento. Qualora il Responsabile ravvisasse la necessità di avvalersi di un altro responsabile del trattamento (Sub responsabile) per l'esecuzione di specifiche attività di trattamento per conto del Titolare, è tenuto a richiederne l'autorizzazione al Titolare con congruo preavviso.
2. Nel caso in cui il Responsabile del trattamento (Responsabile primario) ricorra ad un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile sono imposti, mediante un contratto od un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nella presente Appendice per il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge vigente.
3. Nel caso in cui l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è imputabile.

4. Il Responsabile si impegna a non comunicare, trasferire o condividere, i dati personali trattati per conto del Titolare a Terze parti, salvo qualora legislativamente richiesto e, in ogni caso, informandone preventivamente il Titolare.

Articolo 8 - Misure di sicurezza

1. Il Responsabile, in considerazione della conoscenza maturata in relazione ai progressi tecnici e tecnologici, della natura dei dati personali e delle caratteristiche delle operazioni di trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui alla presente Appendice.
2. Ai fini della sicurezza dei dati e dei sistemi IT, il Responsabile si obbliga:
- ad adottare adeguate misure IT per la sicurezza dei dati personali, ai sensi dell'art. 32 del GDPR, in modo da garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ad adottare adeguate misure che consentano di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- a non trasferire i dati personali oggetto di trattamento per conto del Titolare, senza il preventivo consenso di questi, al di fuori dell'usuale luogo di lavoro, a meno che tale trasferimento non sia autorizzato dalle competenti pubbliche autorità, anche regolamentari e di vigilanza;
- a fornire, in caso di richiesta, al Titolare una descrizione dettagliata delle misure fisiche, tecniche ed organizzative applicate al trattamento dei dati personali;
- ad impiegare sistemi di cifratura per i dati personali memorizzati su dispositivi di archiviazione digitali od elettronici, come computer portatili, CD, dischetti, driver portatili, nastri magnetici o dispositivi similari. I dati personali dovranno essere cifrati nel rispetto della normativa vigente ed il Responsabile dovrà compiere ogni ragionevole sforzo per assicurare l'aggiornamento degli standard di cifratura in modo da tenere il passo dello sviluppo tecnologico e dei rischi ad esso connaturati, includendo ogni richiesta o indicazione emanata da qualsiasi pubblica autorità competente, anche regolamentare e di vigilanza;
- ad adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

Articolo 9 - Registro delle categorie di trattamento

1. Il Responsabile del trattamento adotta, aggiorna e conserva una registrazione scritta di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, avente il contenuto minimo previsto dall'articolo 30, paragrafo 2 del GDPR e, su richiesta, lo rende disponibile all'Autorità di controllo od al Titolare.

Articolo 10 - Violazioni di dati personali

1. In eventuali casi di violazione della sicurezza dei dati personali che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve osservare le disposizioni organizzative contenute nella data breach policy eventualmente adottata dal Titolare e, in ogni caso:
a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire al Titolare tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi. Spetta unicamente al Titolare del trattamento di effettuare la valutazione circa la probabilità di rischio derivante dalla violazione stessa;
b) fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tutte le azioni correttive approvate e/o richieste dal Titolare. Tali

misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito;
2. I Responsabile del trattamento si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 11 - Accordo relativo al trasferimento dei dati all'estero
1. Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei Dati personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server od in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).
2. Il Responsabile, pertanto, non dovrà trasferire od effettuare il Trattamento dei Dati personali del Titolare al di fuori dell'Unione Europea, per nessuna ragione, in assenza di autorizzazione scritta del Titolare. Qualora il Titolare rilasci l'autorizzazione di cui al presente articolo e venga pertanto effettuato un trasferimento dei dati personali del Titolare al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al GDPR sopra indicate. Resta inteso tra le Parti che il Responsabile dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata della presente Appendice. Il Responsabile è obbligato a comunicare immediatamente al Titolare il verificarsi di una delle seguenti fattispecie:
(a) mancato rispetto delle clausole contrattuali standard di cui sopra, oppure
(b) qualsiasi modifica della metodologia e delle finalità trasferimento dei dati personali all'estero.

Articolo 12 - Diritti delle persone interessate
1. È compito del Responsabile del trattamento fornire adeguata informativa agli Interessati dalle operazioni di trattamento, nel momento in cui i dati vengono raccolti.
2. Il Responsabile, per quanto di propria competenza, si obbliga ad assistere ed a supportare il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare riscontro alle richieste per l'esercizio dei diritti dell'Interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile) nel rispetto dei termini previsti dall'art. 12 del GDPR.
3. In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:
- darne tempestiva comunicazione scritta al Titolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate dal Titolare per gestire le relazioni con gli Interessati;

Articolo 13 - Verifiche circa il rispetto delle regole di protezione dei dati personali
1. Il Responsabile riconosce al Titolare il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali per conto del Titolare. A tal fine, il Titolare ha il diritto di disporre – a propria cura e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.
2. Il Responsabile del trattamento fornisce al Titolare tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire al Titolare od a qualsiasi soggetto dal medesimo autorizzato o delegato di condurre audit, comprese le ispezioni, e per contribuire a tali verifiche.
3. Il Responsabile del trattamento deve informare e coinvolgere tempestivamente il Titolare in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 14 - Manleva e Responsabilità per violazione delle disposizioni

1. Il Responsabile s'impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, od altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei dati personali che sia imputabile a fatto, comportamento od omissione del Responsabile (o di suoi dipendenti e/o collaboratori), ivi incluse le eventuali sanzioni che dovessero essere comminate ai sensi del GDPR.
2. Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità alla prestazione dei servizi dedotti nel Contratto.
3. Il Titolare ha il diritto di reclamare dal Responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse dal Responsabile ai sensi dell'art. 82, paragrafo 5, del GDPR.
4. Fatti salvi gli articoli 82, 83, e 84 del GDPR, in caso di violazione delle disposizioni contenute nella presente Appendice, relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute od in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal GDPR, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà direttamente, anche dal punto di vista sanzionatorio.

Articolo 15 - Responsabile della Protezione dei dati personali

1. Il Titolare rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del GDPR, individuando quale soggetto idoneo _____ e che il medesimo è raggiungibile ai seguenti recapiti:

_____

Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.
2. Il Responsabile del trattamento dichiara di aver/non aver provveduto alla nomina del proprio responsabile della protezione dei dati (in caso affermativo, indicarne i dati di contatto).

Articolo 16 – Clausole nulle o inefficaci

1. Qualora una o più clausole della presente Appendice fossero o divenissero contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità della stessa, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'Appendice ove la pura e semplice eliminazione della clausola nulla menomasse gravemente i suoi diritti.

Articolo 17 – Comunicazioni

1. Qualsiasi comunicazione relativa alla presente Appendice ed al sottostante Contratto dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'Appendice. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 18 – Disposizioni finali

1. Per quanto non espressamente indicato nella presente Appendice, il Titolare ed il Responsabile del trattamento rinviano al GDPR, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.