CONSORZIO C.I.S.S-A.C. CALUSO

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 (in lingua inglese) di "*General Data Protection Regulation*" (in italiano, RGPD) 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 e servizi del Consorzio, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

Il trattamento dei dati personali avviene secondo le norme contenute nel **RGPD** nonché nel Decreto Legislativo 30 giugno 2003 (di seguito, per brevità "**Codice privacy**"), così come modificato dal D.Lgs. 10 agosto 2018, n. 101 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*"

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 RGPD, 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 RGPD, 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 RGPD, 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 e di sistemi, mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa del Consorzio, 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 contiene disposizioni organizzative minime, la cui concreta attuazione è demandata alla struttura organizzativa operante all'interno del Consorzio, 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

Il Consorzio 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 ed al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza. In attuazione del suddetto principio il Consorzio 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 RGPD, 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 dell'articolo 5 del RGPD e deve essere in grado di comprovarlo.

La presente disciplina si applica a tutti i dipendenti e collaboratori del Consorzio, individuati quali soggetti designati ed autorizzati ai sensi dell'articolo 2-quaterdecies del Codice privacy, nonché ai responsabili del trattamento ai sensi dell'articolo 28 del RGPD.
Il rispetto delle presenti disposizioni è obbligatorio per tutti i soggetti sopra richiamati e la mancata conformità alle regole di comportamento previste dallo stesso potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero l'applicazione di sanzioni o penali nei confronti delle terze parti inadempienti, secondo le normative vigenti in materia.

Il Consorzio si impegna ad inserire, all'interno degli strumenti di programmazione e pianificazione previsti dalla legge, l'indicazione specifica delle specifiche misure ed iniziative volte ad attuare i principi di protezione dei dati personali.

I.1. 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, il Consorzio sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della protezione dei dati, e migliorare la qualità del servizio.
A tale riguardo, il Consorzio riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale.
Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente o collaboratore 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.
Il Consorzio 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 il Consorzio.
La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

I.2. TRATTAMENTO DEI DATI PERSONALI

Il Consorzio tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali e per l'erogazione dei servizi di propria competenza, quali identificati 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 individuati, 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 il Consorzio 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 all'articolo 30 del RGPD.

I.2.1. Tipologie di dati trattati

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali il Consorzio, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:
• dati personali, quali definiti all'articolo 4, paragrafo 1 del RGPD;
• categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del RGPD (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 RGPD (c.d. dati giudiziari)

I.2.2. Finalità del trattamento

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

I.2.3. Liceità del trattamento

Il Consorzio garantisce che il trattamento dei dati personali avvenga nel rispetto delle condizioni di liceità previsti dalle seguenti disposizioni:
1) articolo 6 del RGPD e 2-ter del Codice privacy;
2) articolo 9 del RGPD, 2-sexies e 2-septies del Codice privacy, in relazione al trattamento delle categorie particolari di dati personali (c.d. dati sensibili e super-sensibili);
3) articolo 10 del RGPD e 2-octies del Codice privacy, in relazione al trattamento dei dati personali relativi a condanne penali e reati

Nel rendere all'interessato le informazioni di cui agli articoli 13 e 14 del RGPD, il Consorzio presta particolare attenzione all'individuazione ed alla illustrazione delle condizioni che legittimano il trattamento.

I.3. CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, Il Consorzio 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 RGPD.
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 RGPD.

I.4. COORDINAMENTO DI NORME

Il Consorzio 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 è prevista la pubblicazione di atti, documenti ed informazioni ed è riconosciuto il diritto di accesso, 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 all'esigenza di protezione dei dati personali è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa consortile, 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" dal Consorzio a trattare i dati personali.

Successivamente alla costruzione sarà, quindi, necessario adeguare le competenze mediante la formazione e l'informazione dei soggetti, abilitando concretamente i soggetti stessi.

II.1. TITOLARE DEL TRATTAMENTO

Articolo 4, n. 7 del RGPD:

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

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

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 RGPD 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 RGPD (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) individuare i contitolari del trattamento e, ove necessario, determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 (art. 26);
e) agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal RGPD (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 in qualità di titolare o di responsabile (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 RGPD (art. 82);
o) rispondere delle violazioni amministrative ai sensi del RGPD (art. 83)

Alla luce del testo normativo e delle interpretazioni correnti, **si ritiene che titolare del trattamento sia il Consorzio 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 esso, nell'ambito delle suddivisioni di ruolo nascenti dal diritto amministrativo.
È fatto salvo quanto previsto da specifiche disposizioni normative che attribuiscano la titolarità del trattamento dei dati personali a figure specifiche.

Le competenze e le responsabilità quali delineate dal RGPD e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi ed al personale del Consorzio in relazione alle funzioni agli stessi assegnati dalla Legge e dallo Statuto.
L'attività gestionale viene svolta, nelle forme e con le modalità prescritte dalla legge, dallo Statuto e dagli appositi regolamenti, dal Direttore coadiuvato dal personale del Consorzio e dal Segretario.
Al Direttore ed ai Responsabili di Uffici e Servizi, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
a) verificare la legittimità dei trattamenti di dati personali effettuati dal Consorzio;
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) adottare soluzioni di privacy by design e by default;
d) contribuire al costante aggiornamento del registro delle attività di trattamento;
e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi adeguate istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
g) disporre l'adozione dei provvedimenti imposti dal Garante;
h) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

i) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
l) adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del RGPD e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del RGPD;
m) garantire al Responsabile della protezione dei dati personali i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
n) 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;
o) consultare il Garante privacy nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del RGPD indichi che il trattamento presenta un rischio residuale elevato;
p) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
q) individuare i responsabili ed i contitolari del trattamento adottando gli atti (accordo sul trattamento dei dati personali ed accordo di contitolarità) e svolgendo le attività, anche di verifica, necessarie.

II.2. PERSONALE AUTORIZZATO AL TRATTAMENTO

Articolo 4, del RGPD
Definizioni
«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le **persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare** o del responsabile

Articolo 29, del RGPD
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 32, del RGPD
Sicurezza del trattamento
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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

Articolo 2-quaterdecies, del Codice privacy
Attribuzione di funzioni e compiti a soggetti designati
2. 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.

L'articolo 29 del RGPD (confermato dal paragrafo 4 dell'articolo 32), in particolare, preso atto dell'eventualità che sotto l'autorità del titolare del trattamento si possano trovare ad operare una o più persone, aventi accesso ai dati personali, si limita a stabilire che le medesime non possano trattare tali dati se non previamente autorizzate ed istruite dal titolare medesimo.
Contrariamente a quanto avvenire nel passato, ad opera dell'articolo 30 del D.Lgs. 30 giugno 2003, n. 196 (nel testo antecedente la modifica apportata dal D.Lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679), il **RGPD** 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*". Analoga previsione è contenuta al paragrafo 4 dell'articolo 32 del RGPD ed è desumibile altresì dalla definizione di "terzo" contenuta nell'articolo 4, n. 10 del RGPD.
In attuazione di ciò, l'articolo 2-quaterdecies del Codice privacy, al comma 2, lascia ampia libertà di forma al titolare per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
Il RGPD e la normativa nazionale di adeguamento consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne alla struttura organizzativa consortile che, ai sensi del Codice

nel testo previgente all'adeguamento al RGPD, ma non anche ai sensi del RGPD, potevano essere definiti come "incaricati".

Il personale operante (a qualunque titolo ed a qualunque livello) all'interno del Consorzio è autorizzato al compimento delle sole operazioni di trattamento di dati personali, necessarie allo svolgimento delle mansioni e funzioni assegnate, sotto l'osservanza delle istruzioni contenute nell'ALLEGATO 1 al presente Modello organizzativo, ovvero di quelle impartite dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto.
L'**autorizzazione**:
• ha validità per l'intera durata del rapporto / incarico;
• viene a cessare al modificarsi del rapporto / incarico;
• viene a cessare in caso di revoca espressa;
• non consente l'attribuzione ad altri soggetti di poteri e compiti previsti;
• al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto di autorizzazione, salvo che ciò sia imposto o consentito da una norma di legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

In fase di prima attuazione del presente Modello Organizzativo il Direttore invia al personale da esso dipendente una comunicazione nella quale si prescrive l'osservanza del presente Modello organizzativo e della procedura di gestione delle violazioni di dati personali (c.d. Data breach policy) e, in particolare, l'osservanza delle istruzioni previste nell'ALLEGATO 1.

In caso di nuove assunzioni si stabilisce che il contratto debba riportare una clausola del seguente tenore (o similare):
"*Il Consorzio si è dotato di un modello organizzativo che, in applicazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo GDPR), individua gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali.*
In attuazione di quanto ivi previsto, è conferita formale ed espressa autorizzazione al trattamento dei soli dati personali necessari allo svolgimento delle funzioni assegnate, con invito al più scrupoloso rispetto della normativa, comunitaria e nazionale, di protezione dei dati personali, oltre alle specifiche istruzioni ed indicazioni operative contenute nel predetto modello organizzativo, applicabili in ragione della posizione ricoperta.
È stato nominato il Responsabile della protezione dei dati personali i cui riferimenti e dati di contatto sono disponibili sul sito web istituzionale dell'Ente."

II.3. DIRETTORE E RESPONSABILE DELL'UFFICIO O SERVIZIO COINVOLTO - DESIGNATO AL TRATTAMENTO

Articolo 2-quaterdecies, del Codice privacy
Attribuzione di funzioni e compiti a soggetti designati
1. 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.

All'interno della struttura organizzativa del Titolare, una fattispecie alquanto peculiare (prevista solo a livello nazionale e non comunitario e sulla quale, in dottrina sussistono non poche perplessità) è quella prevista dal comma 1 dell'articolo 2-quaterdecies del Codice privacy, ove viene prevista la possibilità per il titolare del trattamento di individuare e designare talune persone fisiche alle quali assegnare specifici compiti e funzioni connessi al trattamento di dati personali.

In attuazione del principio per cui i poteri di indirizzo e di controllo politico-amministrativo spettano agli organi di governo, mentre la gestione amministrativa, finanziaria e tecnica è attribuita ai dirigenti (ed assimilati) mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo, si ritiene che le decisioni in ordine alle finalità ed ai mezzi del trattamento, con particolare riferimento alle attività di tipo gestorio, già rientrino nella competenza del Direttore e dei Responsabili di Uffici e Servizi, in relazione al settore di competenza.
Il presente Modello organizzativo intende perseguire l'obiettivo di sintetizzare i principali adempimenti previsti dalla normativa di protezione, offrendo un indirizzo per il riparto delle relative competenze.

Il Consorzio stabilisce che il Direttore e ciascun Responsabile di Uffici e Servizi coinvolto debba essere autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sotto l'osservanza delle istruzioni contenute nell'ALLEGATO 1 al presente Modello organizzativo.

Considerato che al Direttore ed ai Responsabili di Uffici e Servizi spettano l'adozione degli atti e provvedimenti amministrativi, compresi gli atti che impegnano il Consorzio 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 essi sono responsabili, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti, appare **opportuno attribuire loro altresì specifici compiti e funzioni spettanti al Titolare, quali individuati nell'ALLEGATO 2**, ferma restando il generale principio di responsabilità del titolare del trattamento previsto dall'articolo 24 del RGPD.

L'**autorizzazione e la designazione**:
- ha validità per l'intera durata del rapporto / incarico;
- viene a cessare al modificarsi del rapporto / incarico;
- viene a cessare in caso di revoca espressa;
- non consente l'attribuzione ad altri soggetti di poteri e compiti previsti;

• al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto di autorizzazione, salvo che ciò sia imposto o consentito da una norma di legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

II.4. AMMINISTRATORE DI SISTEMA

La figura dell'amministratore di sistema, sebbene non specificamente prevista dal RGPD, svolge un ruolo fondamentale nel garantire il rispetto dei principi di protezione dei dati personali, contribuendo all'attuazione dei principi di "privacy by design" e "privacy by default" (art. 25 del RGPD), di accountability (articolo 5 del RGPD) ed all'adozione di misure di sicurezza adeguate (artt. 24 e 32 del RGPD). I compiti tradizionalmente affidati a tale figura consistono in:
- installazione e configurazione dei sistemi operativi: l'amministratore di sistema è responsabile dell'installazione e della configurazione dei sistemi operativi sui server e sulle workstation. Deve assicurarsi che i sistemi siano correttamente configurati ed ottimizzati per le esigenze del titolare.
- gestione delle reti: l'amministratore di sistema si occupa della gestione e della configurazione delle reti aziendali, compresi i router, gli switch e i firewall. Deve garantire la sicurezza e la stabilità delle reti, nonché l'accesso corretto alle risorse condivise;
- amministrazione dei server: l'amministratore di sistema è responsabile della gestione dei server aziendali, inclusi i server di posta elettronica, i server web, i server di database ed altri server specifici per le esigenze del titolare. Deve assicurarsi che i server siano sempre disponibili, sicuri e performanti;
- gestione degli account utente: l'amministratore di sistema si occupa della gestione degli account utente all'interno delle reti e dei sistemi informativi. Deve creare, modificare e disabilitare gli account utente in base alle esigenze del titolare, garantendo al contempo la sicurezza e l'accesso corretto alle risorse aziendali;
- backup e ripristino dei dati: l'amministratore di sistema deve pianificare e gestire i backup dei dati aziendali, assicurandosi che i dati siano protetti da perdite o danni. In caso di incidenti o guasti, deve essere in grado di ripristinare i dati in modo tempestivo.

Tale figura è stata oggetto di due importanti provvedimenti rilasciati dal Garante per la protezione dei dati personali, rispettivamente del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) e del 25 giugno 2009 (Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento).

Nei provvedimenti del Garante, che continuano ad applicarsi anche a seguito delle modifiche introdotte al Codice privacy dal D.lgs. 101/2018, l'amministratore di sistema è la figura dedicata alla gestione ed alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
La funzione di amministratore è quella di garantire il regolare funzionamento dell'infrastruttura tecnologica aziendale ed il corretto utilizzo della stessa da parte degli utenti interni ed esterni all'organizzazione. Quindi, in virtù di queste sue funzioni, l'amministratore svolge attività che comportano un'effettiva capacità di azione sul dato, anche quando l'amministratore non consulti in chiaro il dato stesso.
Inoltre, lo svolgimento delle mansioni di amministratore di sistema comporta, di regola, la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo

privilegiato a risorse del sistema informativo ed a dati personali cui non si è legittimati ad accedere ad altro titolo.

Per tale motivo, l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono ad incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.
L'obiettivo è quello di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema.
Sulla scorta delle indicazioni fornite dal Garante, si ritiene indispensabile porre la massima attenzione a che:

- l'attribuzione delle funzioni di amministratore di sistema avvenga previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi compresi i profili relativi alla sicurezza;
- la designazione ad amministratore di sistema sia individuale e rechi l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- sia mantenuto un elenco recante i nominativi degli amministratori e delle relative funzioni ad essi attribuite (di sistemi, reti, software).
- siano adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
- l'operato degli amministratori sia oggetto di verifica periodica, almeno annuale, da parte del Direttore, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- nel caso in cui l'attività dell'amministratore di sistema riguardi procedure che determinano il trattamento di dati personali di lavoratori dipendenti, sia resa conoscibile l'identità degli amministratori di sistema nel contesto organizzativo di riferimento;

È demandata alla competenza del Direttore la gestione delle figure di amministratore di sistema affidate al personale appartenente alla struttura organizzativa consortile, nel rispetto dei principi sopra indicati.
Nel caso in cui le attribuzioni di Amministratore di sistema conseguano all'affidamento di servizi tecnologici a soggetti esterni al Consorzio, disposti dal Responsabile di Uffici e Servizi, spetta a quest'ultimo di coinvolgere il Direttore per il coordinamento della relativa gestione.

II.5. CONTITOLARE DEL TRATTAMENTO

Articolo 26, par. 1, del RGPD:
"*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***".

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento. In termini generali, sussiste una contitolarità del trattamento, in relazione a una specifica attività di trattamento, quando soggetti diversi determinano congiuntamente la finalità e i mezzi di tale attività di trattamento.
La valutazione della contitolarità del trattamento dovrebbe essere fondarsi su di un'analisi fattuale, piuttosto che formale, dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento.
È altresì importante sottolineare che un soggetto sarà considerato contitolare del trattamento insieme ad altri solo per quelle operazioni rispetto alle quali determina, insieme agli altri, i mezzi e le finalità di quello stesso trattamento dei dati. Se uno dei soggetti in questione decide isolatamente le finalità e i mezzi delle operazioni precedenti o successive nelle varie fasi del trattamento, tale soggetto deve essere considerato l'unico titolare di tale operazione di trattamento precedente o successiva.
Il fatto che più soggetti siano coinvolti nello stesso trattamento non significa che essi agiscano necessariamente in qualità di contitolari del trattamento.
La qualifica di contitolari del trattamento avrà principalmente conseguenze in termini di ripartizione degli obblighi di rispetto delle norme in materia di protezione dei dati e, in particolare, per quanto concerne i diritti delle persone fisiche. **L'esistenza di una responsabilità congiunta non implica, necessariamente, pari responsabilità**.

Spetta al Direttore ed al Responsabile di Uffici e Servizi coinvolto, anche valendosi della collaborazione del RPD, di identificare gli eventuali contitolari di riferimento e sottoscrivere gli accordi interni per il trattamento dei dati - sulla base delle indicazioni contenute nell'ALLEGATO 3 al presente Modello organizzativo - avendo cura di tenere costantemente aggiornata la relativa documentazione.

A seconda delle circostanze, potrà valutarsi l'adozione delle seguenti misure:

a) 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 dall'accordo. In questo caso, il nominativo ed i dati di contatto del referente interno andranno tempestivamente comunicati all'altra parte;

b) i Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti presentate dagli interessati saranno gestite, 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;

c) 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;

Si ricorda che, a norma dell'articolo 26, par. 2 del RGPD, **il contenuto essenziale dell'accordo di Contitolarità è messo a disposizione degli interessati**. Inoltre, è opportuno richiamare il rapporto di contitolarità all'interno delle informative.

II.6. RESPONSABILE DEL TRATTAMENTO

Articolo 4, n. 8, del RGPD:
"*«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***"

Articolo 28 del RGPD:
"*1. 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.*
2. Il responsabile del trattamento ***non ricorre a un altro responsabile senza previa autorizzazione*** *scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*
3. ***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.*
(…)
9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.
10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione."

Un puntuale approfondimento dei concetti di Titolare, Contitolare e Responsabile del trattamento si rinviene all'interno delle "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR - Versione 2.0*" adottate il 7 luglio 2021 dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), consultabili al seguente indirizzo web:
https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf

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.

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti:
a) **essere un soggetto distinto rispetto al Titolare;**
b) **trattare i dati personali per conto di quest'ultimo**.

Essere "*Un soggetto distinto significa che il titolare del trattamento decide di delegare tutte o parte delle attività di trattamento a un soggetto esterno*". L'esistenza di un Responsabile del trattamento dipende, quindi, 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, pubblica o privata.
"*Il trattamento di dati personali per conto del titolare comporta innanzitutto che il soggetto distinto tratti i dati personali a beneficio del titolare del trattamento*". Il trattamento deve essere effettuato per conto del titolare, ma non agendo sotto la sua autorità o controllo diretti. Agire «per conto di» significa servire gli interessi di terzi e richiama la nozione giuridica di «delega». Nel caso della normativa in materia di protezione dei dati, il responsabile del trattamento è chiamato a seguire le istruzioni impartite dal titolare, almeno per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi. La liceità del trattamento, ai sensi dell'articolo 6 e, se pertinente, dell'articolo 9 del RGPD, deriva dall'attività del titolare del trattamento: il responsabile del trattamento non deve trattare i dati in modo diverso da quanto indicato nelle istruzioni del suddetto titolare. Agire «per conto di» significa, inoltre, che il responsabile del trattamento non può effettuare trattamenti per finalità proprie.
Non tutti i fornitori di servizi che trattano dati personali nel corso della prestazione di detti servizi sono «responsabili del trattamento». In pratica, se il servizio prestato non è destinato specificamente al trattamento di dati personali o se non prevede tale trattamento come un elemento essenziale, il prestatore del servizio può essere in grado di determinare in modo indipendente le finalità e i mezzi di tale trattamento necessario ai fini della prestazione. In siffatta situazione, il prestatore di servizi va considerato come un autonomo titolare del trattamento e non come responsabile dello stesso.
È, pertanto, **necessaria un'analisi caso per caso per stabilire il grado di influenza esercitata da ciascun soggetto nella determinazione delle finalità e dei mezzi del trattamento**.

Spetta al Direttore ed al Responsabile dell'Ufficio o Servizio coinvolto, anche valendosi della collaborazione del RPD, di identificare gli eventuali responsabili del trattamento, valutare l'adeguatezza delle garanzie prestate e sottoscrivere gli accordi sul trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione.

II.6.1. Scelta del responsabile del trattamento

Il titolare del trattamento ha il dovere di impiegare "*unicamente 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 RGPD, anche in merito alla sicurezza dello stesso, e garantisca la tutela dei diritti degli interessati.

Il Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto sono pertanto responsabili della valutazione dell'adeguatezza delle garanzie presentate dal responsabile del trattamento e dovranno essere in grado di dimostrare di aver preso in seria considerazione tutti gli elementi di cui all'articolo 28 del RGPD.

Le garanzie presentate dal responsabile del trattamento sono quelle che il responsabile del trattamento è in grado di dimostrare in modo soddisfacente al titolare del trattamento, essendo queste le uniche che possono essere effettivamente prese in considerazione da detto titolare nel

valutare l'adempimento dei suoi obblighi. Spesso ciò richiederà uno scambio di documentazione pertinente (ad esempio, politica in materia di privacy, condizioni di erogazione del servizio, registro delle attività di trattamento, meccanismi di gestione dei log, politica in materia di sicurezza delle informazioni, relazioni di audit esterni sulla protezione dei dati e certificazioni internazionali riconosciute, come la serie ISO 27000).
La valutazione della sufficienza delle garanzie da parte del Direttore o del Responsabile dell'Ufficio o Servizio coinvolto è una forma di valutazione del rischio che dipenderà in larga misura dal tipo di trattamento affidato al responsabile e va effettuata caso per caso, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche. **Non esiste un elenco esaustivo e predefinito dei documenti o delle attività che il responsabile del trattamento è tenuto a presentare o a dimostrare in un dato caso, in quanto ciò dipende in larga misura dalle circostanze specifiche del trattamento**.

Il Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto dovrebbe tenere conto, almeno, dei seguenti elementi, al fine di valutare l'adeguatezza delle garanzie: le conoscenze specialistiche (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), l'affidabilità e le risorse del responsabile del trattamento. Anche la reputazione del responsabile del trattamento sul mercato può essere un fattore pertinente di cui si può tenere conto.
Inoltre, l'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento in grado di dimostrare garanzie sufficienti.

L'obbligo di impiegare solo responsabili del trattamento «che presentano garanzie sufficienti», ai sensi dell'articolo 28, paragrafo 1, del RGPD è un obbligo permanente. Ad intervalli adeguati, il Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto dovrebbero verificare le garanzie offerte dal responsabile del trattamento, anche, se del caso, mediante attività di revisione e ispezioni.

II.6.2. Forma dell'accordo

Qualsivoglia trattamento di dati personali per conto del Consorzio dev'essere disciplinato da un contratto od altro atto giuridico, concluso tra il titolare e il responsabile del trattamento.
Non è prescritta una specifica forma contrattuale o convenzionale: essa dipenderà dal singolo caso. Ad esempio, potrebbe trattarsi di una convenzione tra enti pubblici o di un contratto nel caso di fornitori privati.
L'accordo sul trattamento deve essere stipulato per iscritto, anche in formato elettronico. Inoltre, il contratto o l'altro atto giuridico deve vincolare il responsabile del trattamento nei confronti del titolare del trattamento, ovverosia deve definire obblighi vincolanti in capo al responsabile del trattamento.
Sebbene l'accordo possa essere integrato in un contratto o convenzione più ampi, l'EDPB raccomanda che gli elementi del contratto volti a dare attuazione all'articolo 28 del RGPD siano chiaramente identificati come tali in un unico punto.

Sia il titolare che il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento. Fatte salve le disposizioni di cui all'articolo 83 del RGPD, l'autorità di controllo competente potrà infliggere una sanzione

amministrativa pecuniaria sia al titolare sia al responsabile del trattamento, tenendo conto delle circostanze di ogni singolo caso.

Valendosi della possibilità prevista dal paragrafo 6 dell'articolo 28 la Commissione Europea, con la decisione di esecuzione 2021/915 del 4 giugno 2021, ha approvato uno **schema di** "**Clausole contrattuali tipo**", consultabili al seguente indirizzo:
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32021D0915

II.6.3. Contenuto dell'accordo

Quanto al contenuto obbligatorio dell'accordo sul trattamento dei dati, l'EDPB interpreta l'articolo 28, paragrafo 3, in modo tale per cui deve esservi stabilito:

- l'oggetto del trattamento (ad esempio, registrazioni di videosorveglianza di persone che entrano o escono da una struttura ad alta sicurezza). Sebbene sia un concetto ampio, esso deve essere formulato con specifiche sufficienti affinché l'oggetto principale del trattamento sia chiaro;
- la durata del trattamento: occorre specificare il periodo di tempo esatto o i criteri utilizzati per determinarlo; ad esempio, si potrebbe fare riferimento alla durata dell'accordo relativo al trattamento;
- la natura del trattamento: il tipo di operazioni eseguite nell'ambito del trattamento (ad esempio: «ripresa», «registrazione», «archiviazione di immagini» ecc.) e la finalità del trattamento (ad esempio: la rilevazione degli ingressi illegittimi). Tale descrizione dovrebbe essere la più completa possibile, a seconda dell'attività di trattamento specifica, in modo da consentire a soggetti esterni (ad esempio le autorità di controllo) di comprendere il contenuto e i rischi del trattamento affidato al relativo responsabile;
- la tipologia di dati personali: questo elemento dovrebbe essere specificato nel modo più dettagliato possibile (ad esempio: le immagini video delle persone che entrano ed escono dalla struttura). Non sarebbe sufficiente limitarsi a specificare che si tratta di «dati personali, ai sensi dell'articolo 4, paragrafo 1, del RGP» o «di categorie particolari di dati personali, ai sensi dell'articolo 9». Nel caso di categorie particolari di dati, il contratto o l'atto giuridico dovrebbero specificare almeno i tipi di dati in questione, ad esempio «informazioni relative alle cartelle cliniche» o «informazioni sull'appartenenza dell'interessato a un sindacato»;
- le categorie di interessati: anche questo aspetto dovrebbe essere indicato in modo piuttosto specifico (ad esempio: «visitatori», «dipendenti», servizi di consegna ecc.);
- gli obblighi ed i diritti del titolare del trattamento: (ad esempio, per quanto riguarda il diritto del titolare del trattamento di effettuare ispezioni e attività di revisione). Quanto agli obblighi del titolare del trattamento, tra gli esempi figurano quello di fornire al responsabile del trattamento i dati di cui al contratto, di fornire e documentare qualsivoglia istruzione relativa al trattamento dei dati da parte del responsabile del trattamento, di garantire, prima e durante l'intero corso del trattamento, l'adempimento degli obblighi di cui al RGPD posti in capo al responsabile, di controllare detto trattamento anche mediante attività di revisione e ispezioni unitamente al suddetto responsabile;
- l'obbligo del responsabile del trattamento di trattare i dati solo su istruzione documentata del titolare del trattamento;
- l'obbligo del responsabile del trattamento di garantire che le persone autorizzate a trattare i dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- l'obbligo del responsabile del trattamento di adottare tutte le misure richieste a norma dell'articolo 32 del RGPD;
- l'obbligo del responsabile del trattamento di rispettare le condizioni di cui all'articolo 28, paragrafo 2, e all'articolo 28, paragrafo 4, per ricorrere a un altro responsabile del trattamento;
- l'obbligo del responsabile del trattamento di assistere il titolare del trattamento nell'adempimento dell'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- l'obbligo del responsabile del trattamento di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD;
- l'obbligo del responsabile del trattamento, al termine della relativa attività, di cancellare o restituire, su scelta del titolare del trattamento, tutti i dati personali al titolare del trattamento e cancellare le copie esistenti;
- l'obbligo del responsabile del trattamento di mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato;

Al fine di garantire un sufficiente livello di omogeneità all'interno della struttura organizzativa consortile, si suggerisce al Direttore ed al Responsabile dell'Ufficio o Servizio coinvolto l'utilizzo della bozza di accordo contenuta nell'ALLEGATO 4, da personalizzare con riferimento al caso di specie.

Il Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto, in relazione ai compiti e/o ai servizi affidati hanno il dovere di **verificare che il soggetto esterno osservi le predette prescrizioni**. La periodicità delle verifiche dovrà essere 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 dovranno registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto e dal Responsabile del trattamento, oltre che dal soggetto che svolge ciascuna verifica.

II.7. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD)

Articolo 38 del RGPD:

*"1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.*

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

*3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. **Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento** o del responsabile del trattamento.*

*4. **Gli interessati possono contattare il responsabile della protezione dei dati** per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.*

*5. Il responsabile della protezione dei dati **è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti,** in conformità del diritto dell'Unione o degli Stati membri.*

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi."

Articolo 39 del RGPD:

*"1. Il responsabile della protezione dei dati è incaricato almeno dei **seguenti compiti**:*

*a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*

*b**) 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;*

*c) fornire, se richiesto, un **parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento** ai sensi dell'articolo 35;*

*d) **cooperare con l'autorità di controllo**; e*

*e) **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

Il Consorzio ha individuato e designato un Responsabile della protezione dei dati (RPD), in possesso di qualità professionali idonee, 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 RPD, pubblicati nel sito web istituzionale del Consorzio, sono comunicati all'Autorità di controllo, ai componenti degli organi di governo, a tutti i dipendenti del Consorzio ed ai componenti degli organi di controllo interni.
I medesimi dati sono inclusi nel contesto delle informazioni rese agli interessati ai sensi degli articoli 13 e 14 del RGPD e delle comunicazioni effettuate ai sensi degli articoli da 15 a 22 e 34 del RGPD.

II.8. REFERENTE DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del RGPD, il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".
Si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal RGPD, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'Ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (RPD), nelle seguenti attività:
a) informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi.
b) sorveglianza dell'osservanza del RGPD, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare 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.
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica;
d) cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.
Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.
Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

PARTE III - ADEMPIMENTI E PROCEDURE

III.1. MISURE PER LA SICUREZZA DEI DATI PERSONALI

Articolo 5 del RGPD:
"1. *I dati personali sono:*
(…)
f) 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 («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)."

Articolo 24, par. 1, del RGPD:
"*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*"

Articolo 32, par. 1, del RGPD:
"*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (…)*"

Il **Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto,** provvedono 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.

III.2. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Articolo 30, par. 1 del RGPD:
"*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. (…)*"

Articolo 30, par. 2 del RGPD:
"*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento (…)*"

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 RGPD e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.
Una grande differenza rispetto a quanto previsto sotto il regime del previgente Codice privacy 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**.

Spetta al Direttore ed al Responsabile dell'Ufficio o Servizio coinvolto, di:
- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, al fine di procedere alla tenuta ed all'aggiornamento del registro;
- effettuare l'aggiornamento periodico, almeno semestrale 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 alla Valutazione d'impatto sulla protezione dei dati personali (DPIA);

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del RPD.
Ai sensi dell'art. 39 del RGPD 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.

Al RPD compete di prestare assistenza al Direttore ed al Responsabile dell'Ufficio o Servizio coinvolto nell'individuazione di:

a) finalità del trattamento;

b) soggetti esterni rispetto ai quali il Consorzio di trovi in una fattispecie di trattamento di dati personali "per conto di" (Responsabile);

c) categorie di destinatari;

d) trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (e relativa adeguatezza);

e) misure di sicurezza;

III.3. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Articolo 35 del RGPD:
"*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua,* ***prima di procedere al trattamento****, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si ***consulta con il responsabile della protezione dei dati****, qualora ne sia designato uno.*
(…)
11. Se necessario, il titolare del trattamento ***procede a un riesame*** *per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*"

Articolo 36, par. 1, del RGPD:
"*Il titolare del trattamento,* ***prima di procedere al trattamento, consulta l'autorità di controllo*** *qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*"

La Valutazione d'impatto sulla protezione dei dati (DPIA) rappresenta una delle principali novità introdotte dalla recente normativa in materia di protezione dei dati personali, in quanto correlata al principio generale di responsabilizzazione del Titolare del trattamento (accountability).
La redazione del documento di valutazione consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli). Più nello specifico il documento illustra le considerazioni logiche che hanno accompagnato le fasi di identificazione, valutazione e risposta a tutti i rischi rilevati all'interno del trattamento oggetto di analisi.
Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.
Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'**articolo 36 del RGPD**, dando luogo alla c.d. consultazione preventiva.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (**articolo 35, paragrafi 1, 3 e 4 del RGPD**), lo svolgimento non corretto di una DPIA (**articolo 35, paragrafi 2, 7 e 9 del RGPD**) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (**articolo 36, paragrafo 3, lettera e) del RGPD** possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro.

III.3.1. Casi di obbligo ed eccezioni

La corretta interpretazione dell'obbligo generale di effettuazione della DPIA è chiarita dalle "**Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01**" adottate dal Gruppo di Lavoro articolo 29 per la protezione dei dati (ora EDPB) il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, il cui testo è raggiungibile al seguente indirizzo web:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Alla luce delle indicate Linee-guida, si ritiene che una valutazione d'impatto sulla protezione dei dati **non sia richiesta nei seguenti casi**:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 119);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. Linee-guida, III.C);
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

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 RGPD.
In particolare, si segnala che **il Garante per la Protezione dei Dati Personali, in data 11 ottobre 2018, ha adottato un "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679"** [doc. web n. 9058979], raggiungibile al seguente indirizzo web:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979

Con particolare riferimento ai trattamenti già esistenti alla data di entrata in vigore del RGPD, le richiamate Linee-guida del Gruppo di Lavoro ex articolo 29 (pag. 15), chiariscono che:

"*L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.*

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal responsabile della protezione dei dati, a norma dell'articolo 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, "[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate" (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati."

III.3.2. Metodologia

I contenuti minimi della DPIA sono specificati come segue dall'**articolo 35, paragrafo 7 del RGPD**:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti 'interessati', si dovrà procedere alla valutazione dell'effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di iniziative finalizzate all'adempimento degli obblighi dettati dal RGPD. Lo schema suggerito è il seguente:
· la descrizione sistematica del trattamento e delle finalità;
· la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
· i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
· una descrizione funzionale dell'operazione di trattamento;
· la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
· la valutazione della necessità e la proporzionalità del trattamento;
· la descrizione delle misure previste per conformarsi al regolamento;
· la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
· la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
· la determinazione delle misure previste per il trattamento di tali rischi;
· la descrizione del modo in cui sono coinvolte le parti interessate;
· il parere del Responsabile della Protezione dei Dati Personali (RPD);
· le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti

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.

La DPIA deve essere effettuata dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto, 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 od il Responsabile dell'Ufficio o Servizio coinvolto garantisce l'effettuazione della DPIA, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno al Consorzio, ed è responsabile della stessa.

Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto **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 devono essere documentate.

Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto 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 RGPD** 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 RGPD; rispetto dei diritti degli interessati di cui al capo III del RGPD);
c. valutazione della obbligatorietà di condurre una DPIA;

Una volta determinata la necessità di procedere ad una attività di DPIA (vedasi il successivo paragrafo III.3.2.) 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 RGPD, 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.
Tutti i documenti prodotti 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 RGPD. 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.
Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto 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 od il Responsabile dell'Ufficio o Servizio coinvolto 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 RGPD, 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 RGPD, anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione consortile, presenza di nuove minacce, ecc.).

Il Responsabile della protezione dei dati personali (RPD) 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 il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto 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.

III.4. VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Il Consorzio adotta 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 il Consorzio (**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 di tale documento è, 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

Articolo 12, par. 2 del RGPD:

"1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento 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 sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

*2. Il **titolare del trattamento agevola l'esercizio dei diritti dell'interessato** ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.*

*3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 **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. Il titolare del trattamento 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.*

*4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento 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.*

*5. **Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento 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 al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

*6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli **dubbi circa l'identità della persona fisica che presenta la richiesta** di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato."*

IV.1. Oggetto ed ambito di applicazione

La presente sezione costituisce adempimento dell'obbligo di agevolare l'esercizio dei diritti previsti dagli articoli da 15 a 22 del RGPD e definisce le attività, i ruoli e le responsabilità che il Consorzio, in qualità di Titolare del trattamento dei dati personali, individua per la gestione delle richieste ricevute da parte dei soggetti interessati per l'esercizio dei propri diritti.

In particolare, rientrano nell'ambito di applicazione della presente disciplina le richieste di esercizio dei diritti riconosciuti dagli articoli da 15 a 22 del GDPR, quali di seguito riassunti:

a) diritto di accesso dell'interessato (articolo 15)
b) diritto di rettifica e cancellazione (articolo 16)
c) diritto alla cancellazione («diritto all'oblio») (articolo 17)
d) diritto di limitazione di trattamento (articolo 18)
e) diritto alla portabilità dei dati (articolo 20)
f) diritto di opposizione (articolo 21)
g) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (articolo 22);

I diritti di cui agli articoli da 15 a 22 del RGPD sono riconosciuti ricorrendo i presupposti previsti nei medesimi articoli ed in applicazione delle deroghe previste dal combinato disposto di cui all'articolo 23 del RGPD ed al Codice privacy, articolo 2-undecies.

Il Consorzio gestirà direttamente tutte le richieste di esercizio dei diritti che pervengano da interessati in relazione a trattamenti rispetto ai quali il Consorzio assume la qualifica di titolare o contitolare del trattamento, anche se ricevute da soggetti terzi individuati ed operanti in qualità di responsabili del trattamento ai sensi dell'articolo 28 del RGPD.

Resta escluso dall'ambito di applicazione della presente disciplina l'esercizio dei diritti che, pur riguardando dati personali, siano disciplinati da specifiche discipline di settore quali, a titolo meramente esemplificativo:
a) Legge 24 agosto 1990, n. 241 (c.d. diritto di accesso documentale);
b) Decreto legislativo 14 marzo 2013, n. 33, articolo 5 (c.d. diritto di accesso civico "semplice");
c) Decreto legislativo 14 marzo 2013, n. 33, articolo 5-bis (c.d. diritto di accesso civico "generalizzato" o "Foia");
d) Decreto Legislativo 19 agosto 2005, n. 195 (c.d. diritto di accesso "ambientale");
e) Decreto del Presidente della Repubblica 30 maggio 1989, n. 223 (Regolamento anagrafico della Popolazione Residente)
f) Decreto del Presidente della Repubblica, 3 Novembre 2000 n. 396 (Ordinamento dello Stato civile);
g) Decreto del Presidente della Repubblica 20 marzo 1967, n. 223, articolo 51 c.d. accesso alle liste elettorali).
Resta, inoltre, escluso dall'ambito di applicazione della presente disciplina, l'esercizio del diritto di reclamo, quale previsto dall'articolo 77 del RGPD e dagli articoli da 140-bis a 143 del Codice privacy.

La segnalazione di fattispecie costituenti violazione di dati personali ai sensi degli articoli 33 e 34 del RGPD va effettuata e viene gestita secondo le norme contenute nella Data Breach policy approvata dal Consorzio.

IV.2. Informazioni sui diritti riconosciuti all'interessato

Le informazioni di cui agli articoli 13 e 14 del RGPD sono fornite dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto, mediante predisposizione di idonea pagina web sul sito istituzionale del Consorzio. Essa contiene tutte le informazioni necessarie a consentire all'interessato di conoscere termini e modalità di esercizio dei propri diritti (c.d. Informativa

privacy). In relazione a specifiche esigenze il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto rende disponibili le informazioni in argomento su supporto cartaceo.
Il RPD sovraintende la predisposizione delle informative e fornisce un modello che garantisca uniformità a tutti gli Uffici e Servizi consortili. Parimenti, spetta al RPD verificare la conformità delle informazioni rese.

Al fine di semplificare la modulistica in uso agli uffici per la raccolta dei dati personali di quanti abbiano relazioni con il Consorzio, si stabilisce che la medesima possa contenere una formulazione riassuntiva delle informazioni previste dal RGPD (**c.d. informativa sintetica o di primo livello**), accompagnata da un rimando espresso alla pagina informativa presente sul sito web istituzionale (**c.d. informativa completa o di secondo livello**).
L'informativa sintetica può essere, altresì, fornita:

- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Consorzio, 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 il Consorzio;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutti i modelli di comunicazioni predisposti dall'Amministrazione e ad essa dirette;
- in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc..

Qualora l'interessato richieda che le informazioni prescritte dagli articoli 13 e 14 del RGPD sia fornite oralmente il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto procede all'identificazione del richiedente, acquisendo gli estremi del documento di identità in corso di validità ed annota la circostanza in apposito verbale da conservare nel rispetto delle norme in materia di documentazione amministrativa.

In attuazione del principio di accountability il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto conserva tutte le versioni delle informative in uno specifico archivio interno cartaceo o telematico e tiene traccia di tutte le modifiche al testo (connesse alle modifiche organizzative, tecniche e normative) al fine di consentire al Consorzio 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.

Qualora il trattamento dei dati personali avvenga ad opera di un responsabile del trattamento e questi raccolga direttamente dati personali presso l'interessato o presso terzi, è tenuto ad informare l'interessato circa la propria condizione di responsabile richiamando, quanto alle informazioni previste dagli articoli 13 e 14, la pagina web sul sito istituzionale del Consorzio.

IV.3. Organizzazione degli uffici

Spetta al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto esaminare e dare seguito alle richieste di esercizio dei diritti, garantendo:
a) l'acquisizione delle richieste in data certa;
b) l'identificazione dell'interessato e del richiedente;
c) la non ricusabilità delle richieste;
d) il tracciamento dei tempi di risposta da parte del Consorzio;
e) la verifica del destinatario della comunicazione e della documentazione prodotta in adempimento alle richieste;
Del ricevimento delle richieste di esercizio dei diritti e degli esiti delle medesime è dato tempestivo avviso al Responsabile della Protezione dei Dati Personali (DPO), il quale fornisce il proprio supporto nella valutazione circa la sussistenza dei presupposti di ammissibilità e nella scelta dei termini e delle procedure di riscontro all'interessato.

Nel caso la richiesta riguardi una o più attività di trattamento svolte da più servizi o settori del Consorzio, il coordinamento dei Responsabili avviene a cura del Direttore. Resta inteso che, l'utilizzo nel presente documento, della terminologia "Responsabile dell'Ufficio o Servizio coinvolto" sta ad indicare altresì la figura del coordinatore di cui sopra.

È istituito un Registro delle richieste di esercizio dei diritti, da tenersi a cura del Direttore o del Responsabile dell'Ufficio o Servizio coinvolto al fine di esaminare e dare seguito alle richieste di esercizio dei diritti, contenente le seguenti informazioni:
a) identificativo univoco della richiesta;
b) dati identificativi e recapiti dell'interessato e dell'eventuale richiedente, se diverso;
c) descrizione sintetica dell'oggetto della richiesta;
d) data di accettazione della richiesta;
e) esito della richiesta;
f) data di comunicazione all'interessato circa l'esito della sua richiesta;
g) note e segnalazioni.
Il registro è tenuto anche allo scopo di valutare eventuali criticità delle procedure di informazione e trattamento dei dati personali nonché al fine di attivare, a seguito dell'apposita valutazione del rischio, le procedure periodiche di audit e verifica dell'adeguatezza delle misure tecniche ed organizzative adottate per il singolo trattamento dei dati ai sensi dell'articolo 32 del GDPR.

Il Direttore ed il Responsabile dell'Ufficio o Servizio coinvolto forniscono **periodica informativa al RPD delle registrazioni effettuate nel Registro delle richieste di esercizio dei diritti**.

La formazione, la gestione e la conservazione della documentazione inerente il procedimento di esercizio dei diritti riconosciuti dall'interessato dal RGPD avviene nel rispetto di quanto previsto dal D.Lgs. 7 marzo 2005, n. 82 (CAD) e relative Linee Guida AgID, dal D.P.R. 28 dicembre 2000 n. 445 (TUDA) e dal D.Lgs. 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio).

La misura del contributo spese previsto dall'articolo 12, paragrafo 5 e dall'articolo 15, paragrafo 3 del RGPD è commisurata a quanto stabilito in materia di accesso ai documenti amministrativi, ai sensi dell'art. 22 della Legge 24 agosto 1990, n. 241.

IV.4. Procedura

IV.4.1. Presentazione della richiesta

Requisito soggettivo per l'esercizio dei diritti di cui trattasi è che la richiesta si riferisca ad informazioni relative a persona fisica, detenute dal Consorzio o che si presume lo siano.
La richiesta dev'essere in forma scritta e va presentata mediante invio agli indirizzi indicati nelle informative di cui al precedente paragrafo IV.2. Essa deve precisare il più possibile l'informazione o le attività di trattamento cui la richiesta si riferisce. **Al fine di agevolare la presentazione della richiesta, dovrà essere reso disponibile sul sito web istituzionale del Consorzio il fac-simile predisposto dall'Autorità Garante della Protezione dei Dati Personali**
(https://www.garanteprivacy.it/documents/10160/10704/MODELLO+esercizio+diritti+in+materia+di+protezione+dei+dati+personali.docx/a356cedc-77b9-4f69-b24b-dadf877bb940?version=1.9).

Richieste di informazione e chiarimento verbali, rivolte agli uffici, sono accoglibili esclusivamente quando comportino il rilascio di informazioni generiche sulle modalità di trattamento dei dati personali adottati dal Consorzio e sulle modalità di esercizio dei diritti dell'Interessato, escludendo tassativamente la comunicazione di ogni altra tipologia di informazione, personale o meno.

La **presentazione della richiesta ad un ufficio incompetente** comporta l'onere per il ricevente di trasmetterla, senza ritardo, all'ufficio competente.
La **presentazione della richiesta ad un responsabile del trattamento** comporta l'onere, per il ricevente, di trasmetterla senza ritardo e, comunque, entro 7 giorni, all'ufficio consortile competente. Contestualmente, il responsabile del trattamento dovrà fornire all'ufficio i dati, le informazioni e tutta la collaborazione necessaria affinché lo stesso possa assolvere al dovere di risposta nei confronti dell'interessato.
Nel caso in cui l'accordo stipulato ai sensi dell'articolo 28 del RGPD preveda la gestione delle richieste dell'interessato come adempimento a carico del responsabile, spetta a quest'ultimo di fornire al competente ufficio tempestiva e documentata notizia circa il ricevimento e l'evasione della stessa.

In caso di presentazione della richiesta al Responsabile della Protezione dei Dati Personali, in quanto punto di contatto ai sensi dell'articolo 38, paragrafo 4, del RGPD, la medesima dovrà essere tempestivamente inoltrata al competente ufficio, dando avviso all'interessato dell'inoltro e dei dati di contatto dell'ufficio competente.

IV.4.2. Identificazione dell'interessato

Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto accerta che la richiesta provenga dal soggetto interessato o da altro soggetto da questi delegato, anche raccogliendo informazioni ulteriori rispetto a quelle contenute nella richiesta, ai sensi e per gli effetti di cui agli articoli 11, paragrafo 2 e 12, paragrafo 6, del RGPD. In particolare:
a) qualora la richiesta provenga direttamente dall'interessato, si procederà alla sua identificazione;
b) qualora la richiesta provenga da parte di un soggetto diverso dall'interessato, incluso un familiare, dovrà essere identificato il richiedente, il quale dovrà produrre apposito atto di delega sottoscritto dall'interessato. La delega non è necessaria nel caso in cui il richiedente eserciti il

diritto per conto di soggetto privo della capacità di agire. In tale caso dovrà essere fornita adeguata documentazione a supporto della richiesta;
c) qualora la richiesta, riguardi una persona deceduta e provenga da chi abbia un interesse proprio o agisca a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione, ai sensi di quanto previsto dall'articolo 2-terdecies del Codice privacy, dovrà essere identificato il richiedente ed acquisita adeguata documentazione a supporto della richiesta.
In relazione alle istanze e dichiarazioni presentate per via telematica, si applica il disposto di cui all'articolo 65 del D.Lgs. 7 marzo 2005, n. 82.

La mancata produzione della documentazione richiesta determina l'improcedibilità della richiesta, qualora il richiedente non ottemperi, entro il termine di 10 giorni, all'invito rivoltogli dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto, con apposita comunicazione. La comunicazione di improcedibilità è inviata entro i 7 giorni successivi e, comunque, nel rispetto del termine previsto dall'articolo 12, paragrafi 3 e 4, del RGPD.

IV.4.3. Esame della richiesta

Ricevuta la richiesta ed effettuata l'identificazione dell'interessato e/o del richiedente Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto individuano il trattamento cui la medesima si riferisce e procede alla relativa istruttoria nell'osservanza dei **criteri** di seguito indicati:
a) verifica circa la presenza dei dati personali negli archivi del Consorzio;
b) individuazione del trattamento oggetto della richiesta;
c) individuazione delle condizioni di liceità del trattamento ai sensi degli articoli 6, 9 e 10 del RGPD;
d) individuazione di altri uffici e servizi, interni al Consorzio, coinvolti nel trattamento;
e) individuazione di soggetti esterni al Consorzio, coinvolti nel trattamento (Responsabili e/o Contitolari);
f) valutazione dell'eventuale carattere di manifesta infondatezza o eccessività della domanda;
g) verifica circa l'esistenza di eventuali criticità nel trattamento o violazioni di dati personali (data breach);
Il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto acquisiscono ogni informazione utile all'istruzione del procedimento, ivi compreso il profilo della competenza ad istruire e decidere, sia rivolgendosi all'interessato che ad altri uffici e servizi del Consorzio.

IV.4.4. Disposizioni relative a specifici diritti

Ove l'interessato presenti una istanza di **accesso ai sensi dell'articolo 15 del RGPD** e questa attenga ad una notevole quantità d'informazioni riguardanti l'interessato il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto lo invitano a precisare, prima che siano fornite le informazioni richieste, a quali dati o attività di trattamento si riferisca l'istanza. In ogni caso, l'esercizio di tale diritto, può riguardare esclusivamente i dati personali e non i documenti che li contengono.
Il diritto d'accesso ai sensi dell'articolo 15 del RGPD può essere esercitato anche più volte e con una cadenza periodica, purché ad intervalli ragionevoli e senza carattere vessatorio.

Ove l'interessato abbia esercitato il **diritto all'integrazione di cui all'articolo 16 del RGPD**, il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto verificano, anzitutto, la necessità di

procedere all'integrazione richiesta nonché la completezza e, ove possibile, la veridicità della dichiarazione integrativa fornita.
Il diritto di rettifica di cui all'articolo 16 del RGPD non può essere esercitato in riferimento ad informazioni di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo.

Nell'ipotesi di esercizio del **diritto di opposizione ai sensi dell'articolo 21 del RGPD**, il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto verificano che l'interessato abbia indicato nell'istanza i motivi connessi alla sua situazione particolare che ne legittimano l'esercizio. La mancata indicazione e documentazione dei motivi determina la non accoglibilità della richiesta, qualora il richiedente non ottemperi, entro il termine di 15 giorni, all'invito rivoltogli dall'Ufficio con apposita comunicazione. La comunicazione di non accoglibilità è inviata entro i 7 giorni successivi.

Il Direttore e ciascun Responsabile dell'Ufficio o Servizio coinvolto, anche avvalendosi dei soggetti di cui all'articolo 28 del RGPD, adottano misure appropriate per consentire di contrassegnare i dati personali presenti nei propri sistemi ICT come "limitati", a seguito di presentazione dell'istanza ai sensi dell'articolo 18 del GDPR.

IV.4.5. Trattamento di dati effettuato in qualità di responsabile o contitolare

In caso di ricevimento di una richiesta di esercizio dei diritti relativa ad un trattamento di dati personali effettuato dal Consorzio nella qualità di responsabile del trattamento il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto:
a) avvia una istruttoria preliminare, al fine di rilevare gli elementi informativi da rendere al titolare, trasmettendogli tempestivamente la richiesta;
b) invia al titolare gli esiti della istruttoria preliminare effettuata, garantendogli tutto il supporto possibile nell'evasione della richiesta;
c) informa l'interessato di aver inoltrato la sua richiesta al titolare del trattamento, il quale sarà competente ad istruire il relativo procedimento ed assumere la necessaria decisione.

Nel caso un soggetto titolare del trattamento abbia ricevuto una istanza di esercizio dei diritti riconosciuti dal RGPD e l'abbia inoltrata al Consorzio quale responsabile del trattamento il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto forniscono al titolare stesso, mediante comunicazione a mezzo PEC e senza ingiustificato ritardo, le informazioni utili o necessarie per consentire il corretto adempimento degli obblighi previsti dagli art. 12-21 del RGPD.

La medesima procedura di cui ai precedenti paragrafi è adottata nel caso in cui il Consorzio sia contitolare del trattamento cui inerisce la richiesta di esercizio dei diritti ma l'accordo interno sottoscritto ai sensi dell'articolo 26 del RGPD preveda in capo ad altro contitolare la competenza alla gestione delle istanze formulate dall'interessato.
Nel caso in cui il Consorzio sia contitolare del trattamento cui inerisce la richiesta di esercizio dei diritti e l'accordo interno sottoscritto ai sensi dell'articolo 26 del RGPD preveda in capo ad esso la competenza alla gestione delle istanze formulate dall'interessato, si osservano le istruzioni previste per l'ipotesi in cui il Consorzio sia (unico) titolare del trattamento, ferma restando la necessità di fornire adeguata informazioni anche agli altri contitolari.

IV.4.6. Riscontro all'interessato

Il riscontro all'interessato deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. La risposta fornita all'interessato deve essere intelligibile, concisa, trasparente, facilmente accessibile, utilizzare un linguaggio semplice e chiaro.

In caso di esercizio del diritto di accesso di cui all'articolo 15, paragrafo 3 del RGPD, il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto forniscono una copia dei dati personali oggetto di trattamento utilizzando modalità che ne garantiscano adeguata sicurezza. In particolare, il riscontro:
a) deve contenere una copia integrale e completa delle sole informazioni richieste, in formato di tipo aperto;
b) non deve recare danno ai diritti ed alle libertà altrui;
c) in caso di trattamento che non prevede l'uso di strumenti elettronici, deve avvenire in busta chiusa, indirizzata all'interessato, anche se la consegna avviene per il tramite di soggetto delegato;
d) in caso di trattamento che prevede l'uso di strumenti elettronici, deve avvenire utilizzando preferibilmente la posta elettronica certificata (PEC), il download diretto dal sito istituzionale del Consorzio od altro strumento di condivisione che presenti adeguate garanzie di sicurezza o supporti non riscrivibili e proteggendo i documenti con password o sottoponendoli a procedure crittografiche. L'uso della crittografia è obbligatorio nel caso di dati personali appartenenti alle categorie particolari di cui agli articoli 9 e 10 del RGPD.

In caso di esercizio del diritto di portabilità di cui all'articolo 20 del RGPD il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto provvedono alla comunicazione dei dati per i quali sussista la condizione di portabilità, in formato aperto, esclusivamente in favore del richiedente, escluso il trasferimento diretto ad altro titolare del trattamento. La trasmissione avviene nel rispetto di quanto previsto al precedente paragrafo.

Qualora, a seguito del suo esame, la richiesta appaia manifestamente infondata o eccessiva, ai sensi dell'articolo 12, paragrafo 5 del RGPD il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto espongono adeguata motivazione nella comunicazione all'interessato, informandolo che l'accoglimento della richiesta è subordinato al pagamento di un contributo spese, determinato ai sensi del precedente paragrafo IV.3.

In caso di diniego opposto alla propria richiesta, l'interessato è sempre informato della possibilità di proporre:
• reclamo all'Autorità Garante per la protezione dei dati personali;
• ricorso giurisdizionale avanti il Tribunale il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.

IV.4.7. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

La comunicazione di cui all'articolo 19 del RGPD è effettuata, tempestivamente, a mezzo di posta elettronica certificata.

IV.4.8. Istanza di riesame al Responsabile della protezione dei dati personali

All'interessato che non ritenga soddisfatto l'esercizio dei diritti, come formulato nella propria istanza ed eventualmente integrato a seguito delle richieste del Direttore o del Responsabile dell'Ufficio o Servizio coinvolto, è assicurata la possibilità di ottenere un riesame ad opera del Responsabile della Protezione dei Dati Personali (RPD).
La comunicazione di riscontro inviata all'interessato ai sensi del precedente paragrafo IV.4.6. contiene, altresì, l'indicazione della facoltà di cui al paragrafo precedente nonché i dati di contatto del Responsabile della Protezione dei Dati Personali.
L'eventuale istanza di riesame indirizzata al Responsabile della Protezione dei Dati Personali è acquisita al protocollo del Consorzio a seguito della sua trasmissione all'Ufficio competente.
Al procedimento di riesame si applica la previsione contenuta al paragrafo 3 dell'articolo 12 del RGPD.
Il Responsabile della Protezione dei Dati Personali che, in occasione della procedura di riesame, riscontri delle non conformità nel trattamento od una immotivata inottemperanza delle richieste di esercizio dei diritti, comunica al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto le azioni correttive o migliorative da adottare (e la relativa tempistica) per assicurare la tutela dei diritti dell'Interessato.

IV.4.9. Informazioni sul trattamento dei dati personali

Il Consorzio, in qualità di titolare del trattamento, tratta i dati personali raccolti in occasione e nel contesto delle procedure per l'esercizio dei diritti, di cui alla presente disciplina, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal GDPR, in particolare per l'esecuzione degli obblighi previsti dalla normativa di protezione dei dati personali, ivi incluse le finalità di trattazione delle istanze pervenute, di archiviazione, di ricerca storica e di analisi per scopi statistici.
Il conferimento dei dati è obbligatorio e la loro mancata indicazione non consente di effettuare l'esame delle istanze. I dati acquisiti nell'ambito della procedura di esame delle istanze saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.
I dati saranno trattati esclusivamente dal personale e da collaboratori del Consorzio o delle imprese espressamente nominate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.
Anche in relazione alle procedure instaurate a seguito della presentazione dell'istanza di esercizio dei diritti riconosciuti dal RGPD, gli interessati hanno il diritto di ottenere dal Consorzio, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza è presentata nelle forme previste dalla presente disciplina.

ALLEGATI

ALLEGATO 1 – “Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali e specifiche istruzioni ai soggetti designati”

ALLEGATO 2 – “Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali e specifiche istruzioni al Direttore ed al Responsabile dell’Ufficio o Servizio coinvolto”

ALLEGATO 3 – “Bozza di accordo di contitolarità”

ALLEGATO 4 – “Bozza di accordo sul trattamento de dati personali”

ALLEGATO 1 - ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI E SPECIFICHE ISTRUZIONI AI SOGGETTI DESIGNATI

Il Consorzio, in forza del principio di «responsabilizzazione», impartisce alla persona fisica individuata ed autorizzata 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, l'autorizzazione ad effettuare le operazioni di trattamento dei dati personali nell'ambito della suddetta attività viene rilasciata a condizione che si rispettino le seguenti istruzioni:

- 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 Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto;
- 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 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 dell'Ufficio o Servizio coinvolto;
  - 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, fatte salve le norme in materia di archiviazione amministrativa. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del RGPD vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato;
- 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 Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto, 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 RGPD e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del RGPD, relative al trattamento attenendosi alle istruzioni ed utilizzando la modulistica all'uopo predisposti dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto;
  - ove si renda necessario, segnalare al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto la necessità di adeguamento, correzione ed integrazione della modulistica in uso all'Ufficio;
  - agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del RGPD. In particolare, qualora riceva richieste provenienti dagli interessati, finalizzate all'esercizio dei propri diritti, dovrà:
    - darne tempestiva comunicazione al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto, allegando copia delle richieste ricevute;
    - coordinarsi, ove necessario e per quanto di propria competenza, con il Direttore od il Responsabile dell'Ufficio o Servizio coinvolto 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 RGPD ed a sostenere i relativi test finali finalizzati alla verifica dell'apprendimento;
- segnalare al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto, 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 Direttore od il Responsabile dell'Ufficio o Servizio coinvolto nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del RGPD, 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 Direttore od il Responsabile dell'Ufficio o Servizio coinvolto nella tenuta del registro delle attività di trattamento istituito ai sensi dell'articolo 30 del RGPD, tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
- segnalare al Direttore od al Responsabile dell'Ufficio o Servizio coinvolto, 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 dal Responsabile dell'Ufficio o Servizio coinvolto 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 od al Responsabile dell'Ufficio o Servizio coinvolto, 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 RGPD;
- 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 Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto o dall'Amministratore di sistema (ove esistente);

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 del Responsabile dell'Ufficio o Servizio coinvolto o dell'Amministratore di sistema (ove esistente).
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 od al Responsabile dell'Ufficio o Servizio coinvolto od all'Amministratore di sistema (ove esistente);
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 il dipendente imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'Amministratore di sistema (ove esistente):

- 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 dipendente;
- deve essere cambiata periodicamente, in conformità alle policies adottate dal Consorzio;
- 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 od il Responsabile dell'Ufficio o Servizio coinvolto può richiedere con apposita e motivata richiesta rivolta all'Amministratore di sistema (ove esistente) 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 od il Responsabile dell'Ufficio o Servizio coinvolto 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 (ad es. 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 dal Responsabile dell'Ufficio o Servizio coinvolto o dell'Amministratore di sistema (ove esistente) 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) il dipendente, 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 standard, 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 del Consorzio, 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 consortile 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 RGPD;
6) non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale del Consorzio 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 od il Responsabile dell'Ufficio o Servizio coinvolto o l'Amministratore di sistema (ove esistente).

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 dal Responsabile dell'Ufficio o Servizio coinvolto o dall'Amministratore di sistema (ove esistente);
2) non è consentito utilizzare 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 RGPD devono essere espressamente autorizzate dal Direttore o dal Responsabile dell'Ufficio o Servizio coinvolto. 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 dell'Ufficio o Servizio coinvolto;
- 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 DIRETTORE ED AL RESPONSABILE DELL'UFFICIO O SERVIZIO COINVOLTO

Ferma restando la necessaria osservanza dei compiti e funzioni di cui al precedente **ALLEGATO 1**, spetta al Direttore ed al Responsabile dell'Ufficio o Servizio coinvolto:

SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

- collaborare con il Direttore e gli altri Responsabili di Uffici o Servizi nell'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 Uffici o Servizi nell'elaborazione e nell'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di violazione dei dati personali (c.d. data breach);
- coordinare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza;
- annotare e mantenere aggiornate le attività di trattamento rilevate, all'interno del registro previsto dall'articolo 30 del RGPD;
- identificare contitolari, responsabili e sub-responsabili di riferimento della struttura organizzativa di competenza e sottoscrivere gli accordi interni e gli accordi sul trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
- acquisire dai contitolari e dai responsabili una dichiarazione dalla quale risulti che le persone fisiche che, presso gli stessi contitolari e responsabili abbiano accesso ai dati personali, siano state autorizzate al trattamento dei dati e siano state istruite in tal senso;
- individuare, 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 propria diretta autorità, impartendo a tale fine analitiche istruzioni, eventualmente integrative di quelle stabilite nel presente Modello organizzativo e controllando costantemente che le persone fisiche individuate 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».
- 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;

- 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 (DPIA);
- 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;
- adottare le misure tecniche ed organizzative adeguate e 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;

- adottare le misure tecniche ed organizzative adeguate 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;

- 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;
- cooperare, su richiesta, con il RPD e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
- osservare le prescrizioni ed adempiere ai compiti previsti nella procedura di gestione delle violazioni di dati personali (data breach policy) adottata dal Consorzio;
- osservare le prescrizioni ed adempiere ai compiti previsti nella Parte IV del presente Modello organizzativo, relativamente ai diritti riconosciuti dal RGPD agli interessati;
- assicurarsi che il RPD sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD nell'esecuzione dei compiti assegnati, fornendogli le risorse necessarie per assolvere tali compiti e per accedere ai dati personali ed ai trattamenti;
- 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 RPD;
- conformare il trattamento ai pareri ed indicazioni del RPD 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;
- programmare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto alla protezione dei dati personali;
- 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 RGPD e della normativa di riferimento.

ALLEGATO 3 - BOZZA DI ACCORDO DI CONTITOLARITA'

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, "RGPD");

3) l'articolo 4, paragrafo 1, n. 7) del RGPD 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 RGPD "*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 RGPD "*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 RGPD, 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 RGPD 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 RGPD;
- 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 RGPD;
- la tenuta dei registri del trattamento ai sensi dell'art. 30 del RGPD;
- 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 RGPD, 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 RGPD 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 RGPD 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 RGPD.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali
1. Nei casi previsti dall'art. 35 del RGPD, 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 RGPD, 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 RGPD 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 RGPD. 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 RGPD; (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 RGPD, 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 RGPD, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.

ALLEGATO 4 - BOZZA DI ACCORDO SUL TRATTAMENTO DE DATI PERSONALI

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI TRA IL TITOLARE E IL RESPONSABILE SECONDO LA DECISIONE DI ESECUZIONE (UE) 2021/915 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo.

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

a) scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) i titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

c) le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) gli allegati da I a IV costituiscono parte integrante delle clausole.

e) le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

f) le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2 - Invariabilità delle clausole

a) le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

a) quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

c) le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 - Clausola di adesione successiva (eventuale)
a) qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
b) una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.
c) l'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento
I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7 - Obblighi delle parti

7.1. Istruzioni
a) il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
b) il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità
Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali
Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento
a) il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello

stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
b) il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili
Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto
a) le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.
b) il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
c) il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.
d) il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
e) su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento
a) Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno 10 giorni prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.
b) qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento),

stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.
c) su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
d) il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.
e) il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali
a) qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.
b) il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento
a) il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.
b) il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.
c) oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei

seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:
1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti 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;
3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.
d) le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali
In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento
In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:
a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2) le probabili conseguenze della violazione dei dati personali;
3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento
In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:
a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III - DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione
a) fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
b) il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.
c) il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.
d) dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la

conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I
ELENCO DELLE PARTI

TITOLARE DEL TRATTAMENTO: [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. DENOMINAZIONE ENTE:

.....

Indirizzo e recapito PEC:

.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....

Firma e data di adesione: .....

N.B.: in caso di contitolarità, indicare gli stessi campi in relazione a tutti i contitolari

** *** **

RESPONSABILE/I DEL TRATTAMENTO [Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

1. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....

Indirizzo e recapito PEC:

.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....

Firma e data di adesione: .....

2. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....

Indirizzo e recapito PEC:

.....

Nome, qualifica e dati di contatto della persona che sottoscrive l'accordo:

.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....

Firma e data di adesione: .....

N.B: In caso di Raggruppamento Temporaneo di Imprese (RTI), vanno indicati anche i mandanti che svolgano attività di trattamento di dati personali per conto del titolare del trattamento.

ALLEGATO II
DESCRIZIONE DEL TRATTAMENTO

Categorie di interessati i cui dati personali sono trattati:

[ ] Dipendenti/Consulenti
[ ] Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] Soggetti che ricoprono cariche sociali
[ ] Beneficiari o assistiti
[ ] Pazienti
[ ] Minori
[ ] Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] Altro (specificare .....)

Categorie di dati personali trattati:

[ ] Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] Dati di profilazione
[ ] Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] Dati relativi all'ubicazione
[ ] Altro (specificare .....)

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari:

[ ] Dati che rivelano l'origine razziale o etnica
[ ] Dati che rivelano le opinioni politiche
[ ] Dati che rivelano le convinzioni religiose o filosofiche
[ ] Dati che rivelano l'appartenenza sindacale
[ ] Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] Dati relativi alla salute
[ ] Dati genetici
[ ] Dati biometrici

Natura del trattamento

.....

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

.....

Durata del trattamento

.....

Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

.....

ALLEGATO III
MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Descrizione delle misure di sicurezza tecniche ed organizzative che devono essere messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

[ ] misure generali
Registro dei trattamenti
Il responsabile del trattamento tiene per iscritto un registro delle attività relative al trattamento svolte per conto del Titolare e delle applicazioni informatizzate utilizzate, nel pieno rispetto del RGPD.
Persone autorizzate
Il Responsabile del Trattamento si impegna a tenere ed aggiornare, in caso di modifiche, l'elenco degli operatori autorizzati ed opportunamente formati in materia di protezione dei dati personali, impartendo loro, per iscritto, specifiche istruzioni su come trattare i dati personali nell'ambito della propria attività, curando, in particolare, il profilo della sicurezza dei dati, ai sensi dell'articolo 29 del RGPD. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.
Persone autorizzate in qualità di Amministratori di Sistema
Il Responsabile, qualora di avvalga di personale che svolga compiti riconducibili a quelli di Amministratori di Sistema, si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità.
Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.
Responsabilità
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 RGPD.
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 presente accordo.
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 RGPD.
Comunicazioni

Qualsiasi comunicazione relativa al presente accordo 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 nell'accordo stesso. Tale indirizzo potrà essere modificato da ciascuna delle parti, dandone comunicazione all'altra ai sensi del presente comma.
Foro competente
Per qualsiasi controversia che dovesse sorgere tra le parti in ordine all'interpretazione del presente accordo e la corretta esecuzione delle disposizioni contrattuali in esso contenute sarà competente il Foro di _____. È esclusa qualsiasi forma di arbitrato.

[ ] procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate, al fine di garantire la sicurezza del trattamento;

[ ] misure per garantire la minimizzazione dei dati quali, a titolo esemplificativo:
- definizione di policy interne che vietino la raccolta di dati non necessari;
- definizione chiara delle finalità: identificare in modo specifico e documentato le finalità per cui i dati personali sono necessari prima di raccoglierli, sulla base di un confronto puntuale con il titolare;
- analisi di necessità e proporzionalità: valutare attentamente se la raccolta di ciascun dato personale sia strettamente necessaria e proporzionata rispetto alle finalità identificate;
- evitare la raccolta di dati "per sicurezza" o "in caso possano servire in futuro";
- limitazione dei dati raccolti: raccogliere solo i dati personali strettamente necessari per le finalità dichiarate. Evitare di raccogliere dati superflui o non pertinenti;
- privacy by design e by default: integrare il principio di minimizzazione dei dati fin dalla progettazione di sistemi, processi e servizi che trattano dati personali, limitando la raccolta e il trattamento dei dati al minimo necessario per impostazione predefinita;
- analisi dettagliata delle effettive necessità di dati per ciascuna attività;
- revisione periodica dei dati raccolti per eliminare quelli superflui;
- formazione del personale sulla minimizzazione dei dati;
- previsione di Audit e controlli interni: eseguire audit e controlli interni per valutare l'implementazione e l'efficacia delle misure di minimizzazione dei dati.

[ ] misure per garantire la qualità dei dati quali, a titolo esemplificativo;
Validazione e Accuratezza dei dati
- implementare procedure di convalida dei dati in fase di inserimento per ridurre errori;
- implementare controlli automatici e/o manuali per controllare la coerenza e l'accuratezza dei dati;
- implementare meccanismi di controllo qualità durante le fasi di elaborazione, migrazione ed archiviazione dei dati per individuare e correggere eventuali errori o incongruenze;
- coinvolgere i dipendenti in sessioni di formazione su tecniche di inserimento corretto dei dati;
-rivedere regolarmente i set di dati per identificare e risolvere discrepanze in modo proattivo;
- implementare sistemi di data quality monitoring;
- implementare processi di escalation per problemi di data quality;
Aggiornamento Periodico dei dati
- stabilire procedure chiare per l'aggiornamento dei dati personali, garantendo che le informazioni trattate siano sempre accurate e attuali;
- programmare attività regolari di aggiornamento per garantire che i dati siano sempre attuali;

- implementare notifiche automatiche per avvisare il personale della necessità di aggiornare informazioni critiche;
- utilizzare procedure di confronto dei dati con il titolare per mantenerne l'attualità;
- stabilire un protocollo per la rimozione o l'archiviazione di dati obsoleti;

Uniformità e Consistenza dei dati

- creare standard di inserimento dei dati per assicurare coerenza in tutta l'organizzazione;
- utilizzare formati predefiniti per dati comuni (es. date, unità di misura) per evitare discrepanze;
- integrare sistemi di gestione dei dati per sincronizzare le informazioni tra diverse piattaforme;
- condurre sessioni di formazione per garantire che i dipendenti comprendano l'importanza della consistenza dei dati.
- monitorare regolarmente i dati per rilevare e correggere incongruenze;

Gestione delle duplicazioni

- definire processi di deduplicazione e pulizia dei dati;
- implementare software di deduplicazione per identificare e unire dati duplicati;
- utilizzare identificatori univoci per garantire che ciascun record nel sistema sia unico;
- eseguire scansioni periodiche per rilevare eventuali duplicati;
- stabilire procedure per la verifica manuale di duplicati segnalati da sistemi automatizzati;
- educare il personale sull'importanza di evitare l'inserimento duplicato di dati.

Formazione del personale sulla gestione dei dati

- organizzare corsi specifici sulle procedure di raccolta e inserimento dati;
- sensibilizzare il personale sull'importanza dell'accuratezza dei dati;
- addestrare il personale all'uso corretto dei sistemi informativi;
- condividere best practices per mantenere alta la qualità dei dati;

[ ] misure per garantire la conservazione limitata dei dati;

- redigere una policy interna che definisca in modo preciso e documentato i tempi di conservazione di ogni tipologia di dato personale trattato per conto del titolare;
- considerare eventuali obblighi legali per la conservazione dei dati, come quelli fiscali o contrattuali;
- documentare le ragioni per eventuali estensioni dei tempi di conservazione;
- applicare una politica di revisione periodica dei termini di conservazione per assicurare la loro attualità;
- evitare di conservare dati oltre il tempo necessario al raggiungimento delle finalità dichiarate;
- implementare sistemi, come scadenziari, sistemi automatici di notifica o flussi di lavoro automatizzati, che permettano di monitorare la data di scadenza dei termini di conservazione ed attivare le procedure di cancellazione o revisione;
- utilizzare database e sistemi di archiviazione che consentano di impostare regole automatiche per la conservazione e la cancellazione dei dati al termine del periodo prestabilito;
- definire processi strutturati di cancellazione;
- utilizzare strumenti certificati di data wiping o ricorrere a fornitori specializzati per la distruzione certificata;
- definire processi di gestione sicura dei supporti di memorizzazione dismessi;
- documentare le operazioni di distruzione dei dati;
- sensibilizzare e formare il personale sull'importanza della conservazione limitata dei dati e sulle procedure aziendali da seguire;
- eseguire verifiche a campione sul rispetto dei tempi di conservazione;

- valutare l'utilizzo di tecniche di pseudonimizzazione o anonimizzazione per ridurre la quantità di dati personali conservati ed il rischio per gli interessati;

[ ] misure per garantire la cancellazione o la restituzione dei dati al termine dell'accordo;
Al termine della prestazione dei servizi relativi al trattamento dei dati personali, il responsabile del trattamento ha l'obbligo di restituire tutti i dati personali al titolare del trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.
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, anche ricorrendo ad una terza parte, a condizione che la terza parte non abbia una relazione competitiva con il Responsabile stesso.
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 del presente accordo, 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
Il responsabile è tenuto 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.

[ ] azioni di Valutazione e Mitigazione dei Rischi quali, a titolo esemplificativo:
- condurre valutazioni per identificare e mitigare i rischi associati ai trattamenti effettuati per conto del titolare;
- adottare procedure interne per valutare la conformità delle pratiche di trattamento dei dati;
- utilizzare strumenti software per monitorare ed analizzare i rischi emergenti e le vulnerabilità;
- collaborare con esperti esterni per condurre audit indipendenti della sicurezza delle informazioni;
- implementare misure correttive tempestive in risposta ai risultati delle valutazioni del rischio;

[ ] misure di gestione degli Accessi ai dati (identificazione e autorizzazione dell'utente) quali, a titolo esemplificativo:
- implementare sistemi di controllo degli accessi basati sui ruoli (RBAC) per garantire che solo il personale autorizzato possa accedere ai dati personali (principio del privilegio minimo);
- stabilire procedure di autorizzazione multilivello per modifiche critiche ai dati;
- utilizzare l'autenticazione multi-fattore (MFA) per aumentare la sicurezza agli accessi;
- revisionare regolarmente i permessi di accesso per accertarsi che siano aggiornati e pertinenti;
- stabilire procedure di revoca degli accessi per dipendenti che abbia cessato il proprio rapporto o trasferiti ad altre posizioni;
- eseguire audit regolari per assicurarsi che le policy di accesso siano rispettate.

[ ] misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati quali, a titolo esemplificativo:
Controllo degli Accessi Fisici

- implementare sistemi di controllo degli accessi come badge elettronici o codici di accesso per limitare l'accesso ai locali dove sono conservati i dati;
- monitorare e registrare chi accede alle aree sensibili attraverso log di accesso che possono essere verificati e revisionati;
- assicurarsi che solo il personale autorizzato possa entrare nelle aree in cui sono presenti dati personali o server;
- installare sistemi di videosorveglianza per monitorare continuamente le aree di accesso critico;
- effettuare controlli periodici per garantire che i dispositivi di accesso siano funzionanti e adeguati alle necessità di sicurezza.

Protezione dei dispositivi hardware

- mantenere un inventario aggiornato di tutti i supporti di memorizzazione (server, hard disk, chiavette USB, ecc.) che contengono dati personali, trattati per conto del titolare, tenendo traccia della loro posizione e del loro utilizzo;
- collocare server ed apparecchiature critiche in armadi o stanze chiuse a chiave per prevenire accessi non autorizzati;
- utilizzare allarmi e sistemi di rilevamento delle intrusioni per segnalare immediatamente accessi non autorizzati o forzature;
- assicurarsi che i dispositivi mobili contenenti dati personali (laptop, smartphone) abbiano misure di sicurezza come blocchi di sicurezza fisici e crittografia dei dati;
- implementare pratiche di gestione del ciclo di vita per dispositivi hardware, comprendendo la tracciabilità e la gestione appropriata dello smaltimento;
- predisporre ed osservare protocolli rigorosi per il trasporto e lo spostamento delle apparecchiature contenenti dati personali;

Protezione delle Strutture

- verificare che le strutture abbiano una protezione adeguata contro incendi, inondazioni e altre calamità naturali;
- installare rilevatori di fumo, sensori d'inondazione e sistemi di estinzione degli incendi per ridurre il rischio di danni fisici ai dati;
- implementare protezioni antisismiche nelle aree soggette a terremoti per prevenire danni strutturali;
- assicurare la tenuta e l'efficienza degli impianti elettrici e di climatizzazione per prevenire interruzioni che possano compromettere l'integrità delle apparecchiature;
- pianificare e testare regolarmente piani di risposta alle emergenze per mitigare l'impatto di disastri fisici;

Gestione dei visitatori

- stabilire politiche chiare per l'accesso dei visitatori alle aree sensibili delle strutture;
- richiedere ai visitatori di firmare registri di ingresso e di essere sempre accompagnati da personale autorizzato;
- fornire badge temporanei per i visitatori per distinguerli facilmente dal personale interno e monitorarne i movimenti;
- limitare le visite a orari specifici e solo alle aree pertinenti alla finalità della visita;
- educare il personale sulle procedure di gestione dei visitatori per garantire la conformità alle politiche aziendali;

[ ] misure di pseudonimizzazione e cifratura dei dati personali quali, a titolo esemplificativo:

- implementare la cifratura dei dati sia in transito che a riposo per proteggerli da accessi non autorizzati (utilizzo di protocolli HTTPS per le comunicazioni web, cifratura del disco rigido dei server che ospitano i dati personali, impiego di VPN per l'accesso remoto);
- utilizzare tecniche di hashing per oscurare gli identificativi diretti;
- utilizzare tecniche di pseudonimizzazione per separare l'identità degli utenti dai dati grezzi;
- cifratura dei database e dei backup;
- assicurarsi che le chiavi di cifratura siano gestite in modo sicuro e accessibili solo al personale autorizzato;
- effettuare audit regolari per verificare l'efficacia delle misure di cifratura;
- formare il personale su come maneggiare dati cifrati e pseudonimizzati, garantendo la loro corretta gestione;
[ ] misure di anonimizzazione dei dati, quando possibile, come l'aggregazione dei dati a livello statistico, la rimozione di informazioni direttamente identificative, ecc.

[ ] misure di protezione dei dati durante la trasmissione quali, a titolo esemplificativo:
- prevedere l'utilizzo di algoritmi di cifratura robusti e riconosciuti (es. AES-256) per la cifratura dei dati in transito;
- definire modalità sicure per lo scambio e la gestione delle chiavi di cifratura, ad esempio tramite protocolli di key agreement o sistemi di gestione delle chiavi centralizzati;
- utilizzare protocolli di cifratura come TLS per le comunicazioni via web (HTTPS);
- implementare della cifratura end-to-end per le comunicazioni e-mail;
- implementare sistemi di cifratura dei dati trasmessi su reti wireless;
- utilizzare VPN per le connessioni remote;
- imporre al proprio personale l'utilizzo di canali di trasmissione sicuri e controllati, limitando o vietando l'utilizzo di metodi di trasmissione non sicuri;
- effettuare una valutazione della sicurezza dei canali utilizzati, considerando fattori come la riservatezza, l'integrità e l'autenticazione;
- prevedere la cifratura dei dispositivi mobili e rimovibili;
- prevedere limitazioni al trasporto fisico di supporti con dati non cifrati;
- prevedere backup cifrati dei dati in transito;
- prevedere la segregazione dei dati personali da altri dati durante la trasmissione, ad esempio tramite l'utilizzo di VLAN dedicate o container crittografati;
- definire misure per proteggere i dati da accessi non autorizzati durante il transito, come l'autenticazione e l'autorizzazione a livello di dispositivo o di applicazione;
- prevedere la registrazione dettagliata di tutti gli accessi e le operazioni sui dati durante la trasmissione, includendo timestamp, utente, indirizzo IP e tipo di operazione;
- implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare il traffico di rete e identificare attività sospette;
- assicurarsi che il personale, coinvolto nella trasmissione dei dati sia adeguatamente formato sulle procedure di sicurezza, sulle policy aziendali e sui rischi connessi alla trasmissione di dati personali;
- definire procedure chiare per la gestione degli incidenti di sicurezza durante la trasmissione dei dati, includendo la segnalazione tempestiva al titolare del trattamento e l'adozione di misure correttive;

[ ] piani di Continuità Operativa e Ripristino dei dati quali, a titolo esemplificativo:
- creare e mantenere aggiornati piani di continuità operativa che includano rapidi tempi di ripristino dei sistemi e dati critici;

- effettuare esercitazioni di simulazione per testare l'efficacia dei piani di continuità e ripristino;
- aggiornare regolarmente i piani di backup per includere nuove risorse e dati critici;
- definire una strategia di backup che preveda sia backup completi periodici che backup incrementali frequenti, in modo da ridurre la perdita di dati in caso di incidente e ottimizzare l'utilizzo dello spazio di archiviazione;
- eseguire regolarmente backup dei dati adottando il principio del "3-2-1": almeno tre copie dei dati; utilizzando almeno due sistemi differenti, di cui una copia deve essere conservata off-site, per assicurare la disponibilità dei dati anche in caso di disastro che comprometta la sede principale;
- utilizzare servizi e piattaforme di backup che rispettino gli standard di protezione dati;
- valutare l'utilizzo di soluzioni di backup che offrano funzionalità di sicurezza avanzate, come la cifratura end-to-end, l'autenticazione a più fattori, la gestione granulare degli accessi e la registrazione di tutte le attività;
- per le macchine virtuali, oltre al backup, effettuare repliche che permettano un rapido ripristino;
- garantire che i supporti di backup fisici e logici e le repliche siano protetti da accessi non autorizzati;
- implementare procedure regolari di revisione e test dei backup per verificare l'integrità e la disponibilità dei dati archiviati;
- prevedere report periodici che attestino l'esecuzione dei backup, l'integrità dei dati e la conformità alle policy definite.
- stabilire procedure di risposta agli incidenti per affrontare rapidamente eventuali violazioni della sicurezza dei dati;
- formare il personale sulle pratiche di gestione delle emergenze e sul loro ruolo nei piani di continuità;

[ ] misure per garantire la registrazione degli eventi informatici quali, a titolo esemplificativo:
Implementazione di Sistemi di Log
- definire le responsabilità in merito alla registrazione degli eventi e collaborare per garantire che i sistemi di log siano in grado di fornire le informazioni necessarie al titolare per l'analisi degli incidenti e la notifica alle autorità competenti;
- implementare sistemi centralizzati che registrino tutti gli eventi rilevanti per la sicurezza ed il trattamento dei dati, come accessi, modifiche, cancellazioni, tentativi di accesso non autorizzati, anomalie
- assicurarsi che i log siano completi e dettagliati, includendo data, ora, utente responsabile e dettagli delle azioni effettuate;
- utilizzare strumenti di correlazione degli eventi;
- eseguire controlli incrociati tra diverse fonti di log;
- predisporre backup regolari dei log per garantirne la disponibilità in caso di necessità di verifica o ripristino;
Determinazione dei Periodi di Conservazione dei Log
- definire chiare politiche di conservazione per i log degli eventi;
- automatizzare i processi di eliminazione dei log scaduti per ridurre il rischio di conservazione eccessiva di dati;
Monitoraggio e Revisione Periodica
- condurre regolari audit dei processi di registrazione degli eventi per assicurare che siano conformi agli standard di sicurezza ed alla normativa di protezione dei dati personali;
- implementare un piano di azione per correggere eventuali discrepanze o lacune identificate durante le revisioni;

- stabilire un sistema di revisione ed auditing dei log per identificare rapidamente eventuali attività sospette;
- documentare tutte le revisioni e le conclusioni per fornire un quadro chiaro delle pratiche di gestione dei log;

Utilizzo di Strumenti di Analytics

- implementare sistemi di monitoraggio in tempo reale che analizzino i log di sistema ed inviino allerte in caso di eventi sospetti o anomalie, consentendo un intervento tempestivo.
- utilizzare dashboard e report per monitorare l'integrità e la sicurezza dei dati continuamente;
- sviluppare indicatori di performance chiave (KPI) per valutare l'efficacia dei sistemi di registrazione degli eventi e l'aderenza alle compliance;

Protezione e Sicurezza dei Dati di Log

- adottare strumenti di sincronizzazione temporale di tutti i sistemi per una corretta cronologia degli eventi
- adottare misure per garantire l'integrità e l'immutabilità dei log, ad esempio tramite firme digitali, sistemi WORM (Write Once Read Many) o blockchain, per evitare la manipolazione o la cancellazione dei dati di log;
- crittografare i dati di log per proteggerli da accessi non autorizzati durante il transito ed a riposo;
- implementare rigide misure di controllo degli accessi per i sistemi di log, assicurando che solo personale qualificato possa visualizzare o modificare i dati;
- testare la sicurezza delle infrastrutture di registrazione degli eventi contro potenziali vulnerabilità;
- definire workflow di escalation per gli eventi rilevanti;
- effettuare simulazioni di incidenti per migliorare le risposte alle situazioni di compromissione dei dati di log;
- eseguire periodicamente revisioni e audit dei sistemi di log per verificarne l'efficacia, l'adeguatezza e la conformità alle normative vigenti;
- attivare procedure e strumenti di analisi forense dei log in caso di incidenti;

Formazione

- formare e sensibilizzazione del personale addetto alla gestione dei sistemi ed alla sicurezza informatica sulle corrette procedure di gestione dei log (lettura ed interpretazione) e sulla loro importanza per l'individuazione e la gestione degli incidenti.

[ ] attività di Formazione e Consapevolezza del Personale:

- organizzare sessioni di formazione regolari per tutto il personale sulla protezione dei dati personali e sulle proprie responsabilità, simulazioni di attacchi informatici e data breach;
- diffondere linee guida e politiche aziendali chiare relative alla gestione dei dati personali;
- sensibilizzare il personale sui rischi legati alla sicurezza informatica e su come prevenirli;
- istituire programmi di aggiornamento continuo per far fronte a cambiamenti normativi e tecnologici;
- monitorare l'efficacia dei programmi di formazione attraverso test e feedback dai partecipanti;

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione ad una violazione di dati personali (data breach):

- attenersi alle prescrizioni contenute nella procedura di gestione delle violazioni di dati personali adottata dal titolare del trattamento;

Comunicazione Tempestiva

- informare tempestivamente il titolare del trattamento una volta rilevata una violazione dei dati personali;
- stabilire canali di comunicazione chiari e diretti con il titolare per garantire una rapida risposta in caso di incidente;

Coordinamento delle Attività di Risposta

- collaborare attivamente con il titolare per valutare l'entità della violazione e le sue potenziali conseguenze;
- partecipare alla stesura e all'esecuzione di un piano di risposta per mitigare i danni e ripristinare la sicurezza;
- eseguire simulazioni e test periodici del piano di risposta agli incidenti per verificarne l'efficacia e garantire che il personale sia pronto ad intervenire in caso di reale necessità;

Documentazione e Reporting

- tenere una documentazione dettagliata di tutti gli aspetti dell'incidente, comprese le cause, le misure adottate e l'interazione con il titolare;
- supportare il titolare nel compilare il registro delle violazioni, necessario per eventuali verifiche da parte del Garante per la protezione dei dati personali;

Implementazione di Misure Correttive

- collaborare con il titolare per identificare ed implementare misure correttive atte a prevenire future violazioni simili;
- partecipare all'aggiornamento delle politiche e procedure di sicurezza in base alle lezioni apprese dall'incidente;

Assistenza nella Notifica al Garante

- fornire al titolare tutte le informazioni necessarie per una tempestiva notifica della violazione al Garante, qualora la violazione possa comportare rischi significativi per i diritti e le libertà delle persone fisiche;
- fornire supporto al titolare del trattamento per l'eventuale comunicazione del data breach all'interessato;

Registro delle violazioni

- mantenere un registro degli incidenti di sicurezza, anche qualora non vi fossero violazioni di dati personali e le medesime non determinassero l'obbligo di notifica all'Autorità di controllo, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del RGPD. A seguito del verificarsi di incidenti di sicurezza, il Titolare potrà:

1. condurre audit, anche senza preavviso e avvalendosi di soggetti terzi;
2. prescrivere ulteriori misure di sicurezza, anche apportando modifiche a quelle previste dal presente accordo;
3. esercitare azioni di rivalsa nei confronti del responsabile;
4. applicare le penali contrattuali;
5. risolvere il contratto in essere con il responsabile.

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione alla Valutazione d'impatto sulla protezione dei dati personali (DPIA):

Collaborazione nella Valutazione dei Rischi

- fornire al titolare una chiara descrizione dei tipi di trattamenti eseguiti e dei dati coinvolti, contribuendo all'identificazione dei possibili rischi;
- supportare il titolare nell'analisi delle specifiche tecniche ed organizzative già esistenti per mitigare tali rischi;

Raccolta e Condivisione delle Informazioni
- garantire la disponibilità di tutte le informazioni necessarie riguardanti le modalità di trattamento ed il workflow dei dati personali;
- contribuire alla raccolta dei feedback e delle osservazioni derivanti dai trattamenti già attivi per affinare l'analisi dei rischi;
- contribuire alla stesura e revisione della documentazione relativa alla DPIA, assicurando che i processi siano chiaramente definiti e completi;
- manutenere registrazioni dettagliate delle discussioni, decisioni e azioni intraprese durante la valutazione d'impatto.
- partecipare alla revisione periodica della DPIA, in un'ottica di miglioramento continuo, offrendo consulenza nelle aree identificate come problematiche o a rischio;
- essere proattivi nell'adeguare misure e procedure in base al feedback raccolto e alle evoluzioni normative;
- supportare il titolare nella comunicazione con l'autorità Garante per la protezione dei dati personali, qualora la DPIA evidenziasse la necessità di una consultazione preventiva;

[ ] misure specifiche in relazione al trasferimento dei dati personali verso Paesi terzi e Organizzazioni internazionali:
Sono vietati i trasferimenti extra SEE verso Paesi terzi e Organizzazioni internazionali.
Salvo che il titolare del trattamento non fornisca, nel presente accordo o successivamente, istruzioni documentate riguardanti il trasferimento dei dati personali verso un paese terzo od una organizzazione internazionale, il responsabile del trattamento non ha diritto di eseguire tale trasferimento.

[ ] misure specifiche che il responsabile del trattamento deve adottare per essere in grado di fornire assistenza al titolare del trattamento in relazione alle istanze di esercizio dei diritti riconosciuti all'interessato:
- rendere all'interessato l'informativa sulla base del modello e delle informazioni fornite dal titolare del trattamento;
- ove necessario, acquisire dall'interessato il consenso al trattamento dei dati personali, sulla base della modulistica e delle informazioni fornite dal titolare;
- conservare, per conto del titolare del trattamento, il consenso espresso dall'interessato, garantendone l'integrità, la disponibilità e la riservatezza;
- fornire al titolare tutte le informazioni necessarie per rispondere alle richieste degli interessati nei tempi previsti dal RGPD;
- inoltrare tempestivamente al titolare tutte le richieste ricevute direttamente dagli interessati, fornendo tutte le informazioni in suo possesso e la documentazione di supporto;
- fornire al titolare il proprio supporto tecnico e specialistico per valutare l'ammissibilità delle richieste e verificare la corretta applicazione del RGPD, in particolare per quanto riguarda le basi giuridiche del trattamento, le eventuali limitazioni all'esercizio dei diritti e le modalità di risposta;
- collaborare attivamente con il titolare per dare seguito alle richieste degli interessati, fornendo l'accesso ai dati, apportando le modifiche richieste od eseguendo le altre operazioni necessarie nel rispetto della normativa e degli accordi contrattuali;
- mettere a disposizione del titolare strumenti e risorse tecniche necessarie per facilitare l'adempimento delle richieste, come meccanismi per l'estrazione e la consegna sicura dei dati;
- implementare tecnologie che permettano la cancellazione o l'anonimizzazione automatizzata dei dati su richiesta;

Qualora il responsabile riceva richieste provenienti dall'interessato, 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 l'interessato.

[ ] misure tecniche ed organizzative specifiche che un eventuale sub-responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento:
- sottoscrivere un accordo scritto con il responsabile principale che definisca chiaramente i compiti, le responsabilità e le misure di sicurezza da adottare. Questo include anche l'obbligo di ricevere autorizzazione scritta dal titolare per eventuali sub-nomine;
- garantire che tutte le operazioni di trattamento rispettino le norme del RGPD e le istruzioni specifiche ricevute dal responsabile principale;
- prevedere audit regolari e verifiche interne per assicurarsi che le politiche di conformità siano efficacemente applicate;
- adottare misure tecniche ed organizzative adeguate per proteggere i dati trattati, come la crittografia, la pseudonimizzazione e restrizioni di accesso, in linea con l'articolo 32 del RGPD;
- assicurare la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- supportare il responsabile principale nel fornire accesso ai dati o rettificarli, cancellarli o limitarli su richiesta degli interessati;
- assistere il responsabile principale nella conduzione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA) se richiesto, fornendo tutta la documentazione necessaria;
- informare immediatamente il responsabile principale di eventuali violazioni della sicurezza che comportino la perdita, la modifica o l'accesso non autorizzato ai dati personali, fornendo tutte le informazioni necessarie per consentire una risposta tempestiva;
- tenere aggiornato un registro delle attività di trattamento per dimostrare la conformità con il RGPD, specificando la natura, la durata, la finalità del trattamento, e le categorie di dati trattati;
- fornire continua formazione al proprio personale sulle normative in materia di protezione dei dati personali e cibersicurezza e sulle migliori pratiche di gestione dei dati;
- mantenersi aggiornato sulle ultime evoluzioni in materia di sicurezza dei dati per migliorare continuamente la protezione;

ALLEGATO IV
ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

NOTA ESPLICATIVA:

Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1].

Il titolare del trattamento ha autorizzato il ricorso ai seguenti sub-responsabili del trattamento:

1. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....

Indirizzo e recapito PEC:

.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento):

.....
.....
.....

2. DENOMINAZIONE ENTE / OPERATORE ECONOMICO:

.....

Indirizzo e recapito PEC:

.....

Nome e dati di contatto del responsabile della protezione dei dati (RPD):

.....
.....

Descrizione del trattamento (compresa una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento):
.....
.....
.....