BOZZA DI ACCORDO SUL TRATTAMENTO DEI 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) AUTORIZZAZIONE PRELIMINARE SPECIFICA: 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 30 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, qualifica e dati di contatto della persona che sottoscrive l'accordo:

……

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):
……
……
……

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):

……

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

Firma e data di adesione: ……