DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE 2023-2024

Istruzione operativa : ADRDT679
Versione : Rif. : VAAS679, DISI679, RMOADS679
Ultima revisione : MIGRAZIONE INCARICHI GDPR-EU/REG.2016/679

Atto di designazione a "Responsabile Delegato al Trattamento" o RDT

Tra

Titolare Designante : .....
Sede Legale Titolare : .....
Codice Fiscale / Partita IVA : .....
Legale Rappresentante : .....

e

RDT Designato : .....
Sede Legale RDT : .....
Codice Fiscale / Partita IVA : .....
Legale Rappresentante RDT : .....

Il Titolare ed il RDT sono di seguito definiti congiuntamente "**Parti**" e in singolo come "**Parte**".

Le parti firmano il cartiglio del presente atto sia in frontespizio e che in calce al documento e considerando l'allegato A - "Istruzioni su diligenze dovute per le misure tecnico-organizzative del trattamento dei dati" in presa visione e accettazione del Designato quale parte integrante del presente Atto a titolo di Privacy Level Agreement (PLA) e Accordi Vincolanti di Impresa (AVI)

Luogo: .....

Data: .....

Titolare del Trattamento

.....

Timbro e firma RDT

Legale Rappresentante

.....

Premesso che:

A. Il Titolare ha affidato all' **RDT** l'erogazione di beni e servizi implicanti il trattamento di dati personali, come meglio descritti nell'Allegato ***A - "Istruzioni su diligenze dovute per le misure tecnico-organizzative del trattamento dei dati"*** o semplicemente **Allegato A**";

B. per trattamento si intende "***qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione***".

C. Il **RDT**, in considerazione:

i) dell'esperienza maturata nell'ambito di riferimento;

ii) della correttezza, sicurezza e professionalità che connota il suo agire imprenditoriale;

iii) della sua organizzazione interna;

iv) della riscontrata mancanza di provvedimenti sanzionatori in materia di protezione dei dati personali

manifesta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate riportate dal Designante nell'Allegato A e per soddisfare i requisiti richiesti dalla normativa vigente in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali Reg. 679/16 (di seguito, la "**Normativa di Riferimento**") e garantisca la tutela dei diritti degli interessati;

D. al fine di ottemperare alle prescrizioni dettate dalla Normativa di Riferimento e di far sì che l'inquadramento dei soggetti coinvolti nelle operazioni di trattamento dei dati personali sia coerente con le predette prescrizioni e normative, il Titolare intende nominare il **RDT**, che l'accetta dichiarando contestualmente di conoscere le istruzioni cui detto Responsabile sarà tenuto ad attenersi nell'espletamento delle attività e servizi affidati.

Le premesse di cui sopra e il contenuto dell'Allegato A, costituiscono parte integrante e sostanziale delle intese raggiunte e delle reciproche pattuizioni, pertanto le Parti convengono quanto segue

1. Oggetto

1.1. Con il presente Atto il Titolare nomina il **RDT** quale "Responsabile del trattamento esterno" dei dati personali che dovrà attenersi alle condizioni indicate nel trattare, per conto del Titolare, i dati secondo finalità, modalità del trattamento, principi di liceità, correttezza, trasparenza, minimizzazione dei dati, all'esattezza, limitazione della conservazione, integrità e riservatezza dei dati, nonché alle misure tecniche e organizzative che dovranno essere adottate al riguardo.

1.2. II Responsabile prende atto che le istruzioni operative di cui all'Allegato A che può essere aggiornato, integrato o modificato in qualunque omento a fronte di eventi sia esterni che interni alla sfera di responsabilità del Titolare e si impegna a rispettarle in tutte le eventuali successive versioni.

1.3. II trattamento dei dati personali dovrà essere effettuato dal Responsabile in conformità a quanto previsto dalla Normativa di Riferimento, dall'Atto e dalle istruzioni impartite dal Titolare esclusivamente per la finalità di diligente e regolare erogazione dei servizi specificamente riportati nel sopracitato Allegato A (di seguito, i "**Servizi**").

1.4. le Parti intendono e applicano le condizioni e le limitazioni di cui in Oggetto quali scritture di tipo Privacy Level Agreement (di seguito **PLA**) e reciproci Accordi Vincolanti di Impresa (di seguito **AVI**), per garantire un'adeguata protezione della vita privata, dei diritti e delle libertà fondamentali degli interessati.

2. Definizioni

Ai fini dell'Atto, i termini indicati con la lettera maiuscola, avranno il significato agli stessi attribuito di seguito. Rimane inteso che ove il contesto della frase lo richieda, i termini definiti al singolare assumeranno il corrispondente significato al plurale e viceversa.

Atto: *indica complessivamente l'accordo attraverso il quale le Parti disciplinano le Diligenze Dovute applicabili al trattamento da parte del Responsabile dei dati personali di cui all'Allegato A*;

Normativa di Riferimento: *indica la normativa nazionale ed europea, anche secondaria, applicabile in materia di trattamento dei dati personali e di libera circolazione di tali dati, come mandatoria per il* ***Regolamento 2016/679*** *(recepito dal GDPR/2016/UE), la legge eventualmente introdotta dagli Stati membri dell'Unione per l'adeguamento delle precedenti produzioni normative in materia al Regolamento, oltre alle Linee Guida del "Gruppo Articolo 29" e le FAQ pubblicate dal Garante per la protezione dei dati personali sul proprio sito istituzionale www.garantepfivacy.it*;

Registro delle attività di trattamento: *ha il significato di cui all'articolo 3. c) dell'Atto;*

Responsabile: *si intende il fornitore a cui il Titolare ha affidato specifiche attività di trattamento di dati personali, nei limiti delle finalità, dei mezzi e delle istruzioni determinate dal Titolare medesimo;*

Servizi e Prestazioni: *indicano l'insieme dei servizi e delle attività che il Titolare ha affidato alla Società e che comportano il trattamento di dati personali di titolarità del Titolare;*

Sub-Responsabili: *ha il significato di cui all'articolo 9.1 dell'Atto;*

Titolare: *indica il Titolare identificato nel frontespizio dell'Atto come Titolare del Trattamento dei Dati Personali (Art.29 Reg. 679/16).*

3. Obblighi del Responsabile

Con il presente Atto, il Responsabile si impegna a:

a. trattare i dati personali esclusivamente per conto del Titolare attenendosi alle istruzioni ricevute, seguendo le clausole e segnalando con tempestività al Titolare le eventuali istruzioni che dovessero risultare non aderenti alla Normativa di Riferimento o che potenzialmente comportino un rischio nel trattamento medesimo;

b. trattare i dati personali di cui all'Allegato A nel pieno rispetto della Normativa di Riferimento, in ragione dei principi applicabili al trattamento dei dati personali, alle condizioni di liceità del trattamento, al consenso prestato dagli interessati ed alle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;

c. effettuare il censimento di tutte le informazioni e di tutte le attività connesse ai Servizi, curanto tutto il ciclo di vita del dato, dalla sua "generazione" nel processo di acquisizione delle informazioni da parte del Titolare, alla sua conservazione all'interno di archivi e/o di banche dati, fino alla sua destinazione finale e la eventuale distruzione. Tali informazioni dovranno essere raccolte all'interno di uno specifico registro (di seguito, il **Registro delle Attività di Trattamento**), contenente, tra l'altro:

   - *il nome e i dati di contatto del Titolare;*
   - *le categorie dei trattamenti effettuati per conto del Titolare;*
   - *dove necessario, l'eventuale trasferimento dei dati personali verso un paese terzo o verso un'organizzazione internazionale, l'identificazione del paese terzo e dell'organizzazione internazionale verso la quale i dati sono stati trasferiti e l'indicazione di ogni documentazione e garanzia volta ad assicurare che il livello di protezione delle persone fisiche all'interno del paese terzo o dell'organizzazione*

internazionale di riferimento non sia pregiudicato (Es. White e Black list con indicazioni di adeguatezza della Commissione europea, l'adesione del destinatario dei dati nel paese terzo o nell'organizzazione internazionale a codici di condotta approvati dalla Commissione europea e/o a meccanismi di certificazione accreditati dalle autorità di controllo competenti, ovvero la formalizzazione di clausole contrattuali adeguate);

- *una descrizione delle misure tecniche e organizzative messe in atto per garantire la sicurezza e l'inviolabilità dei dati personali trattati;*

d. informare tempestivamente il Titolare di tutti gli eventi e le circostanze che potrebbero pregiudicare, per qualsiasi motivo, la sicurezza del trattamento o la capacità di eseguire le obbligazioni in carico al Responsabile;

e. assicurare che dati e informazioni del Titolare siano utilizzati esclusivamente per l'erogazione dei Servizi e siano protetti da adeguate misure di sicurezza fisica e logica volte a garantire che gli stessi restino Integri e non siano in alcun modo e per nessun motivo alterati, smarriti, cancellati, distrutti o comunque resi accessibili a terze parti non autorizzate, manlevando il Titolare da qualsiasi conseguenza o responsabilità;

f. assistere ed affiancare costantemente il Titolare nell'individuazione delle soluzioni informatiche e organizzative più adeguate a garantire l'effettiva protezione degli interessati e nella conduzione della valutazione di impatto dei trattamenti previsti;

g. assicurare che prodotti e servizi tengano conto sin dalla loro progettazione delle regole e dei principi della protezione dei dati personali (**Art.25 Regolamento**), in modo da minimizzarne l'utilizzo e limitare il trattamento ai soli dati necessari al perseguimento delle finalità lecite;

h. prestarsi alle facoltà di verifica e di controllo del Titolare, fornendo tutte le informazioni richieste e predisponendo gli interventi necessari;

i. utilizzare mezzi tecnologici adeguati alle finalità del trattamento richiesto dal Titolare per periodi temporali strettamente necessari al perseguimento delle finalità di cui sopra;

j. nella occorrenza di violazioni di dati personali ed al fine di consentire al Titolare il rispetto delle tempistiche indicate dalla Normativa di Riferimento, informare il Titolare tempestivamente e senza ingiustificato ritardo secondo le modalità e le tempistiche individuate nell'Allegato A, circa anomalie e/o violazioni fornendo collaborazione al Titolare e, se del caso, alle autorità di controllo competenti e coinvolte nello svolgimento delle attività di la notifica della violazione dei dati personali al Titolare e nella quali-quantificazione delle conseguenze.

4. Misure di Sicurezza

4.1. Per tutta la durata del trattamento, il Responsabile si impegna a rispettare quanto previsto dall'Allegato A mettendo in atto ogni altro presidio di sicurezza necessario ad impedire o comunque ridurre al minimo (i) il rischio di distruzione, perdita, diffusione o alterazione dei dati personali ovvero di accidentale o incontrollata consultazione, esportazione, lettura, copiatura degli stessi da parte di terzi, nonché (ii) il rischio di trattamento di dati non consentito o non conforme alle finalità delle operazioni di trattamento, quali, a mero titolo di esempio:

- *la pseudonimizzazione e la cifratura dei dati personali;*
- *la assicurazione, su base permanente, della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi di trattamento;*
- *il ripristino tempestivo della disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;*
- *la redazione e la implementazione di una procedura per monitorare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

4.2. Il Responsabile dovrà periodicamente aggiornare le misure tecniche e organizzative adottate ai sensi dell'Atto, in relazione alle conoscenze acquisite, in base al progresso tecnico, alla natura dei dati, alle specifiche caratteristiche del trattamento e ad eventuali specifici provvedimenti o raccomandazioni di settore. Mediante l'applicazione, in particolare, di quelle misure, nel tempo rese obbligatorie dalla legge ovvero rese disponibili nel settore della sicurezza dei dati personali, previa intesa con il Titolare.

4.3. II Responsabile riconosce e accetta sempre che il Titolare eserciti il diritto di richiedere al Responsabile l'utilizzo di ogni nuova tecnologia, sperimentazione e/o sviluppo tecnologico di cui sia venuto a conoscenza e che sia strettamente funzionale ad una maggiore sicurezza del trattamento.

4.4. Il Responsabile, nell'ambito della propria struttura aziendale, consentirà l'accesso ai dati personali ai soli soggetti che siano stati espressamente autorizzati al trattamento e contestualmente alla loro individuazione e designazione si fa carico di fornire loro specifiche istruzioni circa le modalità di trattamento che siano in linea con quanto disposto dalla Normativa di Riferimento e del presente Atto. Tali soggetti dovranno operare in relazione alle mansioni, le metodologie e gli strumenti di lavoro adeguati all'acquisizione esatta, pertinente e non eccedente dai dati personali, all'eventuale loro aggiornamento, alla conservazione nei termini di legge e, più in generale, ad ogni fase del trattamento e non potranno eseguire operazioni di trattamento per fini diversi rispetto a quelli previsti per l'esecuzione dei Servizi; tutti i trattamenti di cui sopra dovranno essere effettuati entro, e non oltre, il tempo stabilito per ciascuna operazione di trattamento. Laddove i trattamenti dei dati personali dovessero comportare l'uso di sistemi informatici e telematici, l'accesso a tali dati da parte delle persone fisiche autorizzate al trattamento potrà avvenire solo attraverso un opportuno profilo di

abilitazione attivato secondo i criteri e le modalità impartite dal Responsabile (User ID e Password o credenziali definite come da Allegato A). Sarà cura del Responsabile vincolare le persone autorizzate al trattamento ad un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.

4.5. Il Responsabile è anche tenuto alle prescrizioni vigenti in tema di Amministratori di Sistema (ADS), incluso quelle contenute nel Provvedimento del 27 novembre 2008 dall'Autorità Garante per la protezione dei dati personali, recante "*Misure e accorgimenti prescritti ai titolati dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistemi*", poi integrato dal successivo provvedimento datato 29 giugno 2009, con espressa esclusione di qualsiasi effetto sul rapporto di lavoro con il Responsabile. Il Responsabile, si impegna a conservare gli estremi identificativi delle persone fisiche preposte quali ADS e riportandoli prontamente al Titolare se richiesti.

5. Istanze degli interessati

5.1. In caso di ricezione di istanze da parte dagli interessati per l'esercizio dei diritti loro riconosciuti dalla Normativa di Riferimento, il Responsabile dovrà:

- *dare tempestiva comunicazione scritta al Titolare della richiesta ricevuta allegandone copia*
- *tenendo conto della natura del trattamento, assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste degli interessati, nel rispetto delle relative tempistiche e delle scadenze previste dalla Normativa di Riferimento e dell'Allegato A.*

5.2. Dove applicabile, e considerando lle attività di trattamento affidategli, il Responsabile dovrà:

- *permettere al Titolare di fornire agli interessati i dati personali a loro riconducibili in un formato strutturato, di uso comune e leggibile da un dispositivo automatico;*
- *permettere al Titolare di garantire all'interessato i diritti di accesso ai propri dati personali, di rettifica, di opposizione e limitazione del trattamento;*
- *recepire le comunicazioni pervenute dal Titolare con riguardo alle comunicazioni di rettifiche, cancellazioni o limitazioni del trattamento o portabilità dei dati.*

5.3. II Responsabile si impegna a prestare al Titolare analoga collaborazione anche in caso di istanze presentate dalla Autorità di Controllo.

6. Dichiarazioni e garanzie

Il Responsabile dichiara e garantisce di:

a. aver messo in atto misure tecniche ed organizzative adeguate a garantire che il trattamento dei dati personali avvenga nel rispetto della Normativa di Riferimento, anche ai fini della sicurezza del trattamento, fornendo evidenze formali al Titolare su richiesta di quest'ultimo;

b. laddove applicati, aver aderito agli eventuali "**codici di condotta**" compatibili con la propria operatività, registrati e pubblicati dall'autorità di controllo competente e/o dal comitato europeo per la protezione dei dati, e/o di possedere adeguate certificazioni in corso di validità eventualmente rilasciate dagli organismi di certificazione accreditati dall'autorità di controllo competente e/o da organismi di accreditamento idonee a dimostrare la conformità dei trattamenti effettuati alla Normativa di Riferimento; a questo proposito il Responsabile si impegna a mantenere in essere, e a darne evidenza documentale al Titolare, dei suddetti codici di condotta e/o certificati per tutta la durata dell'Atto, sempre assicurando di trasmettere tempestivamente al Titolare una copia degli stessi e di ogni eventuale loro rinnovo, revoca, modifica e/o integrazione;

c. di non essere a conoscenza di condizioni che possano in qualsiasi modo ostacolare o impedire di adempiere alle istruzioni del Titolare o di adempiere agli obblighi di cui al presente Atto.

7. Verifiche e controlli

7.1. Il Responsabile s'impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Atto e della Normativa di Riferimento, anche attraverso la trasmissione, su richiesta del Titolare, di un documento che indichi in maniera dettagliata ed esaustiva le misure tecniche e organizzative adottate. Il Responsabile s'impegna altresì consentire ed a contribuire in ogni momento alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato;

7.2. Il Titolare, direttamente o per il tramite di incaricati di sua fiducia (anche il Responsabile della Protezione dei Dati, RPD se designato), si riserva la facoltà di richiedere a proprio insindacabile giudizio informazioni al Responsabile o di compiere, in qualsiasi momento, verifiche e controlli al fine di accertare la piena conformità del trattamento svolto alle istruzioni impartite. Quindi, il **RDT** riconosce al Titolare, direttamente o per il tramite di propri incaricati di fiducia, nonché all'autorità d controllo, il diritto di accedere a qualsiasi dato personale, a qualsiasi informazione, nonché a qualsiasi locale in cui vengono svolte le operazioni di trattamento e a qualsiasi mezzo o strumento utilizzato per il trattamento dei dati;

7.3. Peraltro, le Parti pattuiscono che i soggetti sopraindicati si impegnano a svolgere le proprie verifiche e i propri controlli per tutto il tempo strettamente necessario, negli orari e con modalità tali da non Interferire con l'attività lavorativa del Responsabile e senza dover corrispondere, né a quest'ultimo né a terzi, alcun compenso di denaro;

7.4. Il Responsabile s'impegna a mettere disposizione del Titolare, del responsabile della protezione dei dati (**RPD**) designato, o dell'autorità di controllo il proprio Registro delle attività di trattamento, su richiesta di questi ultimi;

7.5. Qualora, nel corso della verifica e del controllo, accerti che il Responsabile non ha rispettato le istruzioni impartite, il Titolare potrà fissare un congruo termine entro il quale il Responsabile sarà tenuto ad adeguarsi ai requisiti pattuiti; se decorso inutilmente il tempo concesso, il Titolare avrà facoltà di considerare risolto il rapporto contrattuale con il Responsabile con riferimento al quale sono state svolte le attività di verifica e di controllo.

8. Responsabilità

8.1. II Responsabile risponde con diretta assunzione di responsabilità sia delle violazioni degli obblighi che la Normativa di Riferimento pone a carico dei responsabili del trattamento sia dei comportamenti, anche omissivi, difformi rispetto alle istruzioni impartite dalla Titolare posti in essere dai suoi dipendenti, consulenti e collaboratori, nonché dai dipendenti, consulenti e collaboratori di eventuali fornitori terzi di cui si sia avvalso per l'esecuzione di specifiche attività di trattamento, "***manlevando integralmente il Titolare***" da ogni responsabilità connessa alle suddette violazioni e/o comportamenti. Il Responsabile garantisce di sollevare integralmente e tenere indenni il Titolare, anche ai fini processuali, da qualsiasi onere, danno, spesa o conseguenza pregiudizievole derivante da qualsivoglia azione, eccezione, contestazione o pretesa, giudiziale o extragiudiziale, da chiunque promossa o avanzata per questioni inerenti o conseguenti ad un'eventuale o asserita violazione degli obblighi o delle istruzioni di cui sopra. II Responsabile garantisce altresì di assistere il Titolare affinché siano rispettati gli obblighi relativi alla comunicazione agli interessati e/o all'autorità di controllo della violazione dei dati personali, alla valutazione d'impatto sulla protezione dei dati nonché alla consultazione preventiva.

8.2. Il Titolare risponde con diretta assunzione di responsabilità sia delle violazioni degli obblighi che la Normativa di Riferimento pone a carico dei Titolari del Trattamento sia delle violazioni di dati personali che siano imputabili unicamente alla propria condotta, esonerando integralmente il Responsabile da ogni responsabilità al riguardo.

8.3. Il Responsabile si obbliga ad aderire ai codici di condotta che saranno registrati e pubblicati dall'autorità di controllo competente e/o dal comitato europeo per la protezione dei dati, oppure si adopererà per conseguire le adeguate certificazioni in corso di validità rilasciate dagli organismi di certificazione accreditati dalle autorità di controllo competenti e/o da organismi di accreditamento idonei a dimostrare la conformità dei trattamenti effettuati alla Normativa di Riferimento.

8.4. Quanto sopra da prescrizione, nelle ipotesi in cui il Responsabile determini finalità e mezzi di trattamento in violazioni dell'Atto e della Normativa di Riferimento è egli stesso considerato Titolare del Trattamento.

9. Sub-Responsabile

9.1. Il Titolare conferisce autorizzazione scritta generale al Responsabile per poter ricorrere a eventuali ulteriori soggetti nello svolgimento di specifiche attività di trattamento (di seguito, i "**Sub-Responsabili**").

9.2. Pertanto, il Responsabile si impegna a selezionare **Sub-Responsabili** tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto misure tecniche organizzative adeguate in modo tale che il trattamento svolto da questi ultimi soddisfi i requisiti di cui alla Normativa di Riferimento e garantisca la tutela dei diritti degli interessati ed il rispetto delle istruzioni impartite dal Titolare;

9.3. Il responsabile si impegna in ogni caso a comunicare al Titolare l'intenzione di ricorrere a **Sub-Responsabili**, nonché l'eventuale aggiunta o sostituzione degli stessi, affinchè quest'ultimo abbia l'opportunità preventiva di opporsi;

9.4. Il Responsabile si impegna a stipulare specifici contratti o altri atti giuridici, volti a disciplinare le condizioni e le modalità di trattamento dei dati personali da parte dei **Sub-Responsabili**, che impongano a questi ultimi i medesimi obblighi e le medesime istruzioni a cui egli stesso è tenuto in virtù dell'Atto e ad esibirli a semplice richiesta del Titolare:

9.5. L'autorizzazione di cui al presente articolo consente esclusivamente al Responsabile di procedere autonomamente alla "*formale designazione*" del proprio **Sub-Responsabile** escludento che, in alcun modo, il Responsabile possa ricorrere a "**terze parti**" estranee alla sua organizzazione d'impresa per la fornitura e/o l'erogazione, anche soltanto parziale, dei Servizi "*subappalto*", che continuerà ad essere disciplinata secondo i termini e le condizioni di cui al contratto di riferimento.

9.6. Il Responsabile risponde nei confronti del Titolare dell'operato dei **Sub-Responsabili** se difforme dalla Normativa di Riferimento o dal presente Atto e si impegna a manlevare il Titolare, da qualsiasi danno, pretesa, risarcimento e/o sanzione possa derivare alle medesime, mantenendo su di sé ogni costo, onere o spesa ad esso connesso.

10. Trasferimento internazionale di dati personali

10.1. I dati trattati dal Responsabile in esecuzione dei Servizi non potranno essere da quest'ultimo comunicati a terzi, né diffusi o trasferiti all'estero, salvo quanto eventualmente previsto dalla Normativa di Riferimento. In merito a eventuale trasferimento di dati personali verso paesi terzi all'Unione europea o verso organizzazioni internazionali, il Responsabile potrà trasferire i dati personali esclusivamente verso i paesi terzi o le organizzazioni internazionali nei quali le regole applicabili al trattamento dei dati garantiscono un livello adeguato di protezione delle persone fisiche, sulla base delle valutazioni effettuate dalla Commissione europea.

10.2. Escludento la precedente ipotesi, il Responsabile può procedere al trasferimento dei dati verso paesi terzi all'Unione europea o verso organizzazioni internazionali solo a condizione che disponga di "*adeguate garanzie dei diritti degli interessati*", che il trattamento sia effettuato in "*presenza di norme vincolanti*" per l'impresa destinataria dei dati oppure che sussistano specifiche "*situazioni in deroga*" a quanto sopra, ai sensi della Normativa di Riferimento. Delle suddette valutazioni e garanzie il Responsabile deve dare apposita evidenza al Titolare.

10.3. Qualora il Responsabile non sia stabilito dell'Unione europea, ma tratti dati personali di interessati che si trovino dell'Unione europea, il Responsabile dà atto di aver provveduto a designare per iscritto un "rappresentante nell'Unione Europea" ai sensi della Normativa di Riferimento.

11. Cessazione del trattamento dei dati personali

11.1. Sempre, in caso di cessazione dei Servizi, di scioglimento di questo Atto o di richiesta di cancellazione dei dati personali, il Responsabile dovrà senza ingiustificato ritardo:

a. *restituire al Titolare tutta la documentazione, su qualsiasi supporto, relativa a qualsiasi dato personale di cui sia entrato in possesso nel corso del trattamento o nello svolgimento dell'attività di cui ai richiamati Servizi; la documentazione resa tramite supporti informatici dovrà essere sempre accessibile da parte del Titolare al momento in cui la riceve;*

b. *cancellare, in modo permanente e irreversibile, tutti i dati personali trattati in esecuzione dei Servizi stessi e cancellare le copie esistenti, fatte salve le eventuali "**basi giuridiche**" nazionali e comunitarie che dispongano la conservazione di determinati dati, informazioni e documenti per periodi prefissati. Alle operazioni di cancellazione dei dati predetti dovrà presenziare un incaricato del Titolare, al quale dovrà essere dato preavviso di almeno 7 (sette) giorni lavorativi prima della data di effettuazione di tali operazioni. La cancellazione dovrà essere documentata da apposito verbale, sottoscritto dal Responsabile e dell'incaricato del Titolare.*

11.2. Sempre, al momento della cessazione dei Servizi e/o in caso di scioglimento del contratto che disciplina i Servizi:

a. *relativamente ai Servizi cessati, la presente nomina a Responsabile decadrà contestualmente con effetto immediato, senza necessità di ulteriori formalità o comunicazioni;*

b. *il Responsabile dovrà predisporre, previa richiesta in tal senso da parte del Titolare ed entro 3 (tre) mesi dalla cessazione dei Servizi, una relazione finale circa i trattamenti effettuati nell'esecuzione dei Servizi stessi, le misure di sicurezza adottate, le irregolarità eventualmente riscontrate e le eventuali richieste ricevute dai soggetti interessati e/o dall'autorità di controllo.*

12. Risoluzione

Il Titolare potrà risolvere l'Atto, così risolvendo anche il rapporto contrattuale con il Responsabile ad esso connesso, ai sensi ed agli effetti dell'**art. 1456** del Codice Civile qualora:

a. l'eventuale inadempimento del Responsabile alle istruzioni impartite dal Titolare possa compromettere i diritti degli interessati o la protezione dei loro dati personali;

b. il Responsabile non abbia aderito ai codici di condotta in materia di dati personali o non si sia procurato le certificazioni idonee a dimostrare la conformità dei trattamenti effettuati alla Normativa di Riferimento entro sei mesi dalla loro registrazione e pubblicazione presso l'autorità di controllo competente e/o il comitato europeo per la protezione dei dati;

c. il Responsabile non si sia adeguato alle istruzioni fornite dal Titolare entro i termini di cui al precedente articolo 7.5;

d. il Responsabile abbia trattato i dati personali per finalità ulteriori rispetto a quelle strettamente previste per l'erogazione dei Servizi o non abbia messo in atto adeguate misure di sicurezza fisica e logica volte a garantire che i dati stessi restino integri e non siano in alcun modo e per nessun motivo alterati, smarriti, cancellati, distrutti o comunque resi accessibili a terze parti non autorizzate;

e. il Responsabile abbia violato quanto previsto dall'articolo 10 in materia di trasferimento internazionale di dati personali;

f. il Responsabile abbia violato l'obbligo di informare tempestivamente secondo le modalità e le tempistiche individuate nell'Allegato A, il Titolare di tutti gli eventi e le circostanze che potrebbero pregiudicare, per qualsiasi motivo, la sicurezza del trattamento o la capacità di eseguire, o di eseguire nei tempi previsti, le sue diligenze dovute.

13. Referenti delle Parti

Ai fini del presente Atto, il Titolare dichiara di non avere al momento designato un proprio Responsabile della protezione dei dati (di seguito "Data Protection Officer o, in breve, "**DPO**" o "**RPD**").

Qualora dovessero mutare le condizioni di obbligatorietà o se il Titolare dovesse volontariamente designarlo, i dati di contatto saranno riportati sul proprio sito web quindi disponibili anche al Responsabile. Eventuali aggiornamenti e/o modifiche dei suddetti dati di contatto che possano rilevare nei rapporti Titolare/Responsabile saranno messi a disposizione del Responsabile da parte del Titolare con le stesse modalità.

Per garantire la migliore gestione possibile degli obblighi di cui al presente Atto e consentire al Titolare di svolgere le verifiche ed i controlli di propria competenza, il Responsabile mette a disposizione del Titolare i dati di contatto del proprio DPO, se designato, o di altro soggetto che nell'ambito dell'organizzazione aziendale del Responsabile è deputato a gestire le tematiche in ambito privacy e protezione dei dati ai sensi del Regolamento.

Eventuali aggiornamenti e/o modifiche dei dati di contatto del soggetto citato che possano rilevare nei rapporti Responsabile/Titolare saranno messi a disposizione del Titolare da parte del Responsabile con le modalità discrezionali preventivamente concordate tra le Parti.

14. Disposizioni varie

14.1. Il presente Atto è produttivo di effetti per tutta la durata dei Servizi, fermo restando l'obbligo in capo al Responsabile, anche successivamente alla cessazione dei Servizi stessi, di mantenere riservati tutti i dati conosciuti in esecuzione dei medesimi e di osservare la Normativa di Riferimento.

14.2. Il presente Atto è da considerarsi riservato e confidenziale e non può essere né diffuso né comunicato a terzi senza il consenso scritto del Titolare.

14.3. Le Parti concordano che l'Atto è a titolo gratuito e che l'attribuzione alla Società del ruolo di Responsabile non potrà comportare in capo al Titolare alcun aggravio dei costi concordati per l'esecuzione dei Servizi.

14.4. In merito a questioni relative al trattamento dei dati personali, l'Atto prevale sulle eventuali disposizioni contrastanti contenute all'interno del contratto volto a disciplinare i Servizi.

14.5. L'Atto è regolato e deve essere interpretato secondo la legge italiana. Per ogni controversia che dovesse sorgere in ordine alla validità, efficacia, interpretazione,

esecuzione e scioglimento dell'Atto sarà competente in via esclusiva il Foro geograficamente associato al Titolare

Letto, confermato e sottoscritto per accettazione.

Luogo: .....

Data: .....

Amministratore di Sistema

come da Politica Privacy

Timbro e firma RDT

Legale Rappresentante

.....

.....

Titolare del Trattamento

.....

CLAUSOLE COMPROMISSORIE

Ai sensi e per gli effetti dell'articolo 1341 e 1342 del codice civile, il Responsabile dichiara di aver riletto attentamente e compreso, nonché di approvare espressamente, le seguenti disposizioni contenute all'interno dell'Atto: 8.1 (manleva in favore del Titolare per eventuali danni derivanti da pretese o azioni di terzi intentate a seguito di inadempimenti alle obbligazioni di cui all'Atto ed alla Normativa di Riferimento da parte del Responsabile e/o di qualsiasi altro soggetto del cui operato debba rispondere, nonché per qualsiasi costo, spesa, onere connessi); 9 (nomina da parte del Responsabile di eventuali Sub-Responsabili); 10 (divieto di trasferimento di dati qualora il paese terzo all'Unione europea o l'organizzazione internazionale di destinazione non garantiscano un adeguato livello di protezione degli interessati),12 (facoltà di risoluzione espressa dell'Atto e del contratto di appalto di riferimento); 14.5 (legge applicabile e foro competente).

ALLEGATO A

Istruzioni su diligenze dovute per le misure tecnico-organizzative del trattamento dei dati in carico al Responsabile del Trattamento esterno

La Normativa di Riferimento impone ai soggetti coinvolti nelle operazioni di trattamento di dati personali di mettere in atto misure tecniche ed organizzative che garantiscano un adeguato livello di sicurezza dei dati personali e di adottare processi strutturati di rilevazione, di notifica e di comunicazione delle violazioni di sicurezza comportanti l'accidentale e/o l'illecita distruzione, perdita, modifica, divulgazione di tali dati o l'accesso non autorizzato ai dati medesimi.

Obiettivo del presente Allegato A è quello di fornire al Responsabile le istruzioni di trattamento cui attenersi nell'ambito dell'erogazione dei Servizi richiesti dal Titolare. Tali istruzioni dovranno essere recepite dal Responsabile che si impegna a svolgere ogni intervento necessario al rispetto a) *delle istruzioni*, b) *a mantenere un appropriato livello di sicurezza del trattamento* e c) *ad assistere il Titolare nell'individuare le soluzioni tecniche ed organizzative adeguate ed efficaci in funzione del trattamento concretamente svolto*.

1. MISURE DI SICUREZZA

I trattamenti di dati personali di cui ai Servizi dovranno essere posti in essere dal Responsabile nel pieno rispetto delle prescrizioni della Normativa di Riferimento non escludento il riferimento ai principi applicabili al trattamento dei dati personali, all'adozione delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e tenendo conto dei provvedimenti tempo per tempo emanati ed aggiornati dal Garante per la protezione dei dati personali o da altre autorità di controllo competenti in materia di protezione dei dati personali.

Il Responsabile dichiara e garantisce che il trattamento di cui all'Atto (cDoc: **ADADSext679**):

- sarà effettuato sia manualmente sia con l'ausilio di strumenti elettronici o comunque automatizzati e per via telematica, con modalità strettamente correlate alle finalità dei trattamenti da effettuare;
- si attuerà per il tempo e con le modalità strettamente necessarie al perseguimento delle finalità del trattamento tali da garantire la riservatezza, integrità e disponibilità dei dati personali;
- sarà effettuato soltanto dopo aver messo in atto le misure adeguate a ridurre al minimo i rischi di:
  - *distruzione, perdita e violazione, anche accidentale, dei dati stessi;*
  - *accesso, in modo accidentale o illegale, ai dati personali;*
  - *modifica e divulgazione non autorizzata dei dati personali;*
  - *trattamento non autorizzato o illecito dei dati personali.*

Nel valutare l'adeguatezza delle misure di sicurezza messe in atto, il Responsabile dovrà tenere conto in special modo dei predetti rischi insiti nel trattamento.

Le misure di sicurezza adottate ai sensi dell' Atto di Designazione dovranno essere periodicamente aggiornate dal Responsabile — *in relazione alla conoscenze tempo per tempo dal medesimo acquisite in base al progresso tecnico, alla natura dei dati, alle specifiche caratteristiche del trattamento e ad eventuali specifici provvedimenti o raccomandazioni di settore* — mediante l'applicazione, in particolare, di quelle ulteriori o rafforzate misure aggiornate, rese obbligatorie dalla legge o comunque rese disponibili nel settore della sicurezza dei dati personali, previa Intesa con il Titolare.

Il Responsabile, inoltre, sarà tenuto a:

- implementare le proprie misure di sicurezza secondo i principi di "Privacy by design" e "Privacy by default"
- adottare misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio a cui i dati, i trattamenti, i diritti e le libertà delle persone fisiche sono esposti, tenuto conto delle indicazioni fornite dal Titolare anche a seguito dell'analisi di impatto effettuata (**DPIA**);
- garantire la continua riservatezza, integrità e disponibilità dei dati stessi, impartendo istruzioni tecniche e organizzative per la corretta custodia e utilizzo dei supporti rimovibili di memorizzazione, attraverso le Politiche Privacy e Protezioone dei Dati interne alla organizzazione del Titolare.
- mettere in atto procedure interne volte a testare, verificare e valutare che le misure tecniche e organizzative implementate garantiscano la sicurezza del trattamento;
- comunicare e trasmettere al Titolare la documentazione tecnica relativa alle modifiche, tempo per tempo apportate alle misure di sicurezza adottate in riferimento al trattamento dei dati oggetto dei Servizi;
- garantire la disponibilità e la resilienza dei sistemi e dei Servizi, ripristinando tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, definendo delle misure tecniche e di processo per il corretto backup dei dati personali e prevedendo attività periodiche di test volte a verificare il restore dei dati.

2. MISURE PER TRATTAMENTO EFFETTUATO CON STRUMENTI ELETTRONICI

Sistemi di Autenticazione e/o Autorizzazione informatica

Il Responsabile deve far sì che:

- il trattamento di dati personali con strumenti elettronici sia consentito alle sole persone autorizzate dotate di credenziali che consentano il superamento di una procedura di autenticazione e/ o autorizzazione relativa a uno specifico trattamento o a un insieme di trattamenti;
- l' autenticazione e/ o autorizzazione informatica delle persone autorizzate al trattamento sia effettuata tramite un codice identificativo personale associato ad una parola chiave riservata conosciuta solamente dalle medesime o tramite il sistema ritenuto più adeguato al livello di rischio rilevato per lo specifico trattamento;
- il sistema di autenticazione e/ o autorizzazione informatica garantisca che ogni persona autorizzata al trattamento di dati personali veda assegnata o associata individualmente una o più credenziali per l' autenticazione e/ o autorizzazione;
- siano impartite alle persone autorizzate al trattamento di dati personali istruzioni sulle cautele per la segretezza della password e sulla diligente custodia degli eventuali dispositivi in possesso ed uso esclusivo di queste ultime;
- la password sia composta dal numero (non inferiore ad 8) e da una tipologia di caratteri ritenuti adeguati al rischio rilevato per lo specifico trattamento;
- siano impartite istruzioni affinché le password non siano facilmente riconducibili alle persone autorizzate al trattamento di dati personali;
- la password sia modificata dalla persona autorizzata al trattamento di dati personali al primo utilizzo e, successivamente, **almeno ogni tre mesi**. Nel caso in cui le persone siano autorizzate al trattamento di particolari categorie di dati personali, la password dovrà essere modificata almeno ogni tre mesi;
- il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altre persone, neppure in tempi diversi;
- le credenziali di autenticazione e/ o autorizzazione (eccetto le utenze tecniche sistemistiche degli ADS o dello *staff* informatico abilitato) vengano disattivate dopo un periodo di inutilizzo ritenuto adeguato rispetto al rischio rilevato;
- le credenziali di autenticazione e/ o autorizzazione vengano disabilitate in caso di perdita della qualità che consente alla persona autorizzata l'accesso ai dati personali (es. cambi di ruolo);
- siano impartite istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante la sessione di trattamento;

- siano presenti le disposizioni relative ai casi di assenza prolungata della persona autorizzata al trattamento, in relazione alla custodia delle copie delle credenziali.

Condizioni specifiche per le Autorizzazioni

Il Responsabile deve far sì che:

- quando per le persone autorizzate al trattamento di dati personali sono individuati profili di autorizzazione di ambito diverso, sia utilizzato un sistema di autorizzazione;
- il sistema di autorizzazione sia configurato in modo tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni del trattamento (principio del minimo privilegio)
- la sussistenza delle condizioni per il mantenimento dei profili autorizzativi sia verificata con periodicità almeno annuale.

Altre misure di sicurezza

Il Responsabile deve far sì che:

- nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito alle persone autorizzate al trattamento di dati personali e addette alla gestione o alla manutenzione degli strumenti elettronici, la lista di queste persone possa essere redatta anche per categorie di incarico e dei relativi profili di autorizzazione;
- i dati personali siano protetti contro il rischio di intrusione e dell'azione di programmi di cui all'Art615-quinquies del codice penale, mediante adeguati strumenti elettronici (es. firewall, TDS, antivirus) aggiornati almeno ogni 6 mesi;
- gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti siano effettuati almeno annualmente. In caso di trattamento di "***categorie particolari***" di dati personali l'aggiornamento deve essere almeno semestrale;
- siano impartite istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale;

Per le prassi e le contromisure IT che all'interno della organizzazione del Titolare sono già in carico all'ADS, il Responsabile dovrà comunque coordinare le attività di cui sopra e verificarle

Ulteriori misure in caso di trattamento di dati particolari (ex art. 9 GDPR)

Il Responsabile deve far sì che:

- i dati personali che rientrino in ***categorie particolari*** siano protetti contro l'accesso abusivo, di cui all'Art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici;
- siano impartite istruzioni tecniche e organizzative per la corretta custodia e utilizzo dei supporti rimovibili di memorizzazione e dei dispositivi mobili in dotazione di Soggetti Autorizzati se utilizzati in modo promisquo con accesso alla rete interna;
- siano impartite istruzioni per la distruzione dei supporti rimovibili contenenti categorie particolari di dati personali non più utilizzati e per la distruzione di tali dati dai supporti riutilizzati da altri addetti non autorizzati al trattamento di dati personali;
- siano adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

3. MISURE PER I TRATTAMENTI CARTACEI

Per il trattamento effettuato senza l'ausilio di strumenti elettronici, il Responsabile deve:

- impartire alle persone autorizzate al trattamento di dati personali istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- far sì che nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito alle persone autorizzate al trattamento di dati personali, la lista di queste persone possa essere redatta anche per categorie di incarico e dei relativi profili di autorizzazione;
- far sì che quando gli atti e i documenti contenenti ***categorie particolari*** di dati personali (ex art. 9 GDPR), sono affidati a determinate persone per lo svolgimento dei relativi compiti, i medesimi atti e documenti siano controllati e custoditi da queste persone fino alla loro restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e siano restituiti al termine delle operazioni affidate;
- garantire che l'accesso fisico ai locali e agli archivi contenenti categorie particolari di dati sia controllato;
- adottare procedure idonee a far sì che le persone ammesse all'accesso ai locali dell'azienda, a qualunque titolo, dopo l'orario di chiusura, siano identificate e registrate;
- quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi, garantire che le persone che vi accedono siano preventivamente autorizzate.

4. MISURE CONCERNENTI LE PERSONE AUTORIZZATE AL TRATTAMENTO DI DATI PERSONALI

Il Responsabile deve:

- far sì che le persone autorizzate al trattamento di dati personali abbiano accesso e trattino esclusivamente i dati personali che sono strettamente necessari per dare corretta e piena esecuzione ai Servizi o per adempiere ad obblighi di legge e, in ogni caso, nei limiti e in conformità con i termini dell'Atto e della Normativa di Riferimento,
- consentire il trattamento dei dati personali unicamente alle persone che:
  - i. *per esperienza, capacità e formazione risultano idonee ad assicurare il rispetto della Normativa di Riferimento;*
  - ii. *abbiano svolto con cadenza almeno annuale un corso di formazione circa gli obblighi disposti dalla Normativa di Riferimento;*
  - iii. *siano state autorizzate per iscritto allo svolgimento di operazioni di trattamento di dati personali.*

Mediante l'autorizzazione di cui sopra il Responsabile deve altresì impartire per iscritto alle suddette persone dettagliate istruzioni operative relative agli obblighi a cui sono tenute nel trattamento dei dati personali, alle precauzioni che le medesime devono adottare per garantire che il trattamento dei dati personali si svolga in conformità all'Atto ed alla Normativa di Riferimento ed alle attività da compiere in caso di violazione dei dati personali.

Il Responsabile deve altresì:

- vigilare scrupolosamente sugli adempimenti, da parte delle Soggetti Autorizzati (SSAA) al trattamento di dati personali, delle istruzioni ricevute e degli obblighi da questi sottoscritti;
- approntare misure fisiche, tecniche ed organizzative che ogni soggetto autorizzato al trattamento possa avere accesso esclusivamente ai Dati Personali che possono essere trattati in base al proprio profilo di autorizzazione, sula base dell'attività che devono compiere nell'esecuzione dei Servizi;
- far sì che le persone autorizzate al trattamento mantengano un comportamento conforme a quanto previsto nell'atto e nella normativa di riferimento e comunque improntato a standard di diligenza, correttezza e professionalità, astenendosi da qualsiasi condotta, attiva od omissiva, che possa violare la Normativa di Riferimento o che possa determinare conseguenze pregiudizievoli per il Titolare;
- far sì che il personale esterno non dipendente del Responsabile sia autorizzato al trattamento, nei limiti in cui la legge o il contratto di riferimento lo consentano, per il solo periodo necessario all'erogazione dei Servizi. Tali soggetti dovranno operare sotto la diretta responsabilità del Responsabile;

5. MISURE CONCERNENTI GLI AMMINISTRATORI DI SISTEMA

Se del caso, il Responsabile è tenuto a designare gli amministratori di sistema (ADS) e rispettare quanto indicato nel provvedimento generale del Garante 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 successivo Provvedimento del 25 giugno 2009, recante "*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*".

Il Responsabile dovrà predisporre, aggiornare e conservare l'elenco contenente gli estremi identificativi delle persone fisiche preposte quali ADS e comunicare al Titolare, a richiesta di quest'ultimo e comunque con periodicità almeno annuale, l'elenco aggiornato degli ADS, specificando in una apposita lista quali siano gli ADS che nell'ambito delle proprie funzioni e mansioni abbiano la possibilità di intervenire sui dati personali di pertinenza o comunque in possesso del Titolare.

Il Responsabile dovrà inoltre verificare annualmente l'operato degli ADS in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Il Responsabile deve adottare sistemi di sicurezza adeguati alla registrazione degli accessi logici (sia HW che SW) ai sistemi di elaborazione e agli archivi elettronici da parte degli ADS. Tali registrazioni (collezioni di log digitali) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono inoltre comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a 6 (sei) mesi.

6. VIOLAZIONE DEI DATI PERSONALI (Data Breach)

In presenza di violazioni, anche solo presunte, di dati personali, il Responsabile è tenuto a:

a) informare il Titolare, nella persona del DPO se designato, immediatamente e comunque entro 24 ore da quanto ha avuto conoscenza dell'evento, inviando una comunicazione redatta sulla base del modulo di seguito riportato e fornendo le informazioni ivi indicate;

b) di concerto con il Titolare, adottare immediatamente o comunque senza ingiustificato ritardo ogni necessaria misura volta a minimizzare i rischi di qualsivoglia natura per i dati personali e porre in essere ogni eventuale operazione necessaria per porre rimedio alla violazione dei dati personali, per attenuarne i possibili effetti negativi e per investigarne la causa.

Il Responsabile deve inoltre tenere un registro che elenchi le violazioni dei dati personali, le circostanze ad esse relative, le conseguenze di ciascuna violazione, i provvedimenti adottati per porvi rimedio. Tale registro dovrà essere esibito al Titolare a semplice richiesta di quest'ultimo.

Per la gestione del Dossier "Data Breach" il Titolare ha predisposto i seguenti documenti del Manuale **SPPS**:

RG-DB01 Garante Infografica Data Breach, FS-DB679NAG-Modello segnalazione data breach PA, IO-DB01-IstruzioneOperativa DataBreach, RV-DB01-RegistroViolazioniDataBreach DB-PG679-ProcGestionale-DataBreach

In questo contesto si riportano le informazioni indispensabili contenute nella relazione conclusiva di un evento di "Data Breach" cosi come riportata nel Registro delle Violazioni

- ***Soggetto che compila il modulo relativo alla violazione dei dati personali***
- ***Nome della società (ivi compresi eventuali collaboratori) che ha rilevato la violazione dei dati personali***
- ***Natura della violazione dei dati personali***
- ***Data e orario in cui la violazione dei dati si è verificata***
- ***Data e orario in cui si è venuti a conoscenza della violazione dei dati***
- ***Categorie e numero approssimativo di interessati i cui dati personali sono stato oggetto della violazione***
- ***Categorie e numero approssimativo di dati personali oggetto della violazione***
- ***Stato/i membro/i di provenienza dei dati personali oggetto della violazione dei dati personali***
- ***Nome e dati di contatto del Responsabile della Protezione dei Dati, se previsto***
- ***Probabili conseguenze della violazione dei dati personali***
- ***Misure a disposizione per porre rimedio e/o per attenuare i possibili effetti negativi della violazione dei dati personali***
- ***Eventuali commenti finali***

7. DIRITTI DEGLI INTERESSATI

Il Responsabile dichiara e garantisce di aver adottato misure tecniche e organizzative adeguate per consentire l'esercizio dei diritti degli interessati ai sensi della Normativa di Riferimento, impegnandosi a evadere qualsiasi richiesta formulata da parte del Titolare per far fronte alle richieste degli interessati.

Il Responsabile si obbliga a collaborare con il Titolare per garantire che le richieste di esercizio dei diritti degli interessati previsti dalla Normativa di Riferimento siano soddisfatte entro i tempi e secondo le modalità di legge.

Il termine previsto per l'evasione operativa della richiesta formulata dal Titolare non deve in ogni caso superare i 5 giorni solari dal momento della formulazione della stessa.

Il Responsabile dovrà garantire l'effettivo esercizio dei diritti riconosciuti agli interessati dalla Normativa di Riferimento sulla base degli accordi intercorsi con il Titolare, impegnandosi a notificare per iscritto al Titolare entro un termine di 5 giorni solari qualsivoglia richiesta di esercizio di tali diritti formulata direttamente da parte degli interessati, allegando altresì una copia della richiesta.

8. SCHEMA DI RIFERIMENTO PER SERVIZI E CATEGORIE DI DATI

Per la gestione delle diligenze dovute del RDT, il Titolare fornisce il seguente schema semplificato del Manuale **SPPS**

Gli ambiti di trattamento e Servizi di riferimento convenuti tra Titolare e Responsabile sono riassunti in modo non esaustivo le seguenti categorie di dati :

Dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato) direttamente o indirettamente.

Dati personali comuni

- **Anagrafici** - Dati personali anagrafici quali nome, cognome, data e luogo di nascita, stato civile, residenza.
- **contabili, fiscali, inerenti possidenze e riscossione** - Dati personali quali versioni parziali/integrali di documenti contabili, dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore, indicazioni di dati riferiti a percettori di somme (e.g. i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti).
  - **inerenti il rapporto di lavoro** - Dati personali inerenti l'esecuzione del rapporto di lavoro: tipologia di contratto e livello contrattuale, dettagli di assunzione, stipendio, etc.
  - **tracciamenti** Dati personali presenti nei tracciati record generati dalla registrazione delle operazioni svolte su sistemi, applicativi, ecc.
- **Dati personali finanziari**
  - dati relativi all'esistenza di rapporti finanziari - Dati relativi alla situazione bancaria attuale e/o passata dell'interessato, informazioni gestite da operatori finanziari quali: i saldi iniziali e finali del rapporto, il totale dei movimenti annuali in entrata e in uscita, la c.d. giacenza annuale media etc. (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)
- **Dati personali sensibili** - convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
  - Dati personali che possano rivelare convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

- **Dati personali ultrasensibili** - stato di salute, assistenza sanitaria, orientamento/vita sessuale
    - Sottoinsieme di dati sensibili attinenti: - lo stato di salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, dati idonei a rivelare informazioni relative al suo stato di salute, ad esempio, certificato medico, cartella clinica, etc.

- **Dati personali giudiziari**

- **casellario giudiziale** - Dati contenuti all'interno del certificato penale del casellario giudiziale.

- **qualità di indagato/imputato o altre situazioni giudiziarie e reati o connesse misure di sicurezza**
    - Dati idonei a rivelare che un determinato soggetto è stato sottoposto ad indagini di polizia giudiziaria, al termine delle quali, è stato accusato di un reato nell'ambito di un Procedimento penale (certificato dei carichi pendenti)

Altri esempi: provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione