ALLEGATO

A.ADDT

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 RDTE, 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