NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Premessa

L'attività che S.S.C. (di seguito Fornitore o Responsabile) svolge a favore dell'impresa associata (di seguito Titolare del trattamento) comporta la conoscenza, da parte del Fornitore, dei dati personali che sono oggetto di tutela da parte del Regolamento (UE) 2016/679 (di seguito anche il "Regolamento") e del Dlg. 196/03 s. m. i. (di seguito, insieme, anche "normativa privacy"): il trattamento dei dati personali è 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.

1. Nomina

L'impresa associata nomina, pertanto Apa Servizi srl **Responsabile del trattamento dei dati personali** ai sensi della Normativa Privacy per i dati personali e per la realizzazione dei servizi dettagliati nel contratto tra le parti (di cui la presente nomina è parte integrante) e sintetizzati in allegato I.

La presente nomina viene conferita anche per la funzione di Amministratore di Sistema. Per gli adempimenti connessi alla realizzazione delle funzioni di Amministratore di Sistema si rinvia alle istruzioni contenute nell'allegato III al presente atto di nomina.

Tutte le informazioni a cui il Responsabile avrà eventualmente accesso in qualità di Responsabile del trattamento debbono essere considerate informazioni aziendali riservate.

2. Le competenze in materia di protezione dei dati personali

La sottoscrizione del presente atto da parte del Responsabile implica anche il riconoscimento della sussistenza di idonea competenza in materia di protezione dei dati personali ossia della conoscenza dei principi della normativa a tutela dei dati personali nonché delle cognizioni in materia di sicurezza dei dati personali.

3. Ambito di trattamento e finalità

Il Titolare del trattamento e il Responsabile del trattamento sottoscrivono il presente documento al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

Le istruzioni contenute nel presente documento (atto di nomina) si applicano al trattamento dei dati personali specificato all'allegato I.

Gli allegati da I a III costituiscono parte integrante del presente atto.

Il Responsabile tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato I, salvo ulteriori istruzioni del Titolare 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 I.

4. Poteri

Con il presente atto viene conferito il potere al Responsabile di individuare le persone autorizzate al trattamento e di dare loro istruzioni scritte in conformità alla normativa privacy e alle specifiche disposizioni delle Autorità di Controllo (ai sensi dell'art 51 del Regolamento).

Le persone autorizzate che opereranno sotto la diretta responsabilità del Responsabile avranno il compito di effettuare tutte le operazioni ritenute necessarie per l'espletamento delle funzioni previste dalla normativa privacy.

L'elenco con i nominativi delle persone autorizzate al trattamento completo e aggiornato dovrà essere fornito dal Responsabile al Titolare del trattamento laddove quest'ultimo ne facesse richiesta. Resta fermo che la responsabilità per eventuali mancati o non corretti adempimenti alla normativa privacy da parte di tali soggetti ricadrà interamente sul Responsabile.

5. Istruzioni

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.

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 personali.

Il Responsabile supporta il Titolare in caso di interazione con il Garante per la protezione dei dati personali o con altre Autorità in caso di richieste di informazioni o effettuazione di controlli e accessi da parte di quest'ultime.

Oltre alle istruzioni indicate nel presente atto, le ulteriori istruzioni disciplinate nel contratto stipulato tra il Titolare e il Responsabile si intendono qui integralmente riportate e accettate.

6. Persone autorizzate

a) Il Responsabile del trattamento dichiara che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

b) Il Responsabile del trattamento dichiara che le persone autorizzate al trattamento dei dati personali hanno frequentato un corso di formazione sui principi del Regolamento e sulle misure di sicurezza da adottare.

7. Misure di sicurezza

a) Il Responsabile del trattamento assiste il Titolare del trattamento nel garantire il rispetto degli obblighi relativi alla sicurezza del trattamento (ai sensi dell'articolo 32 del Regolamento);

b) 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 personali (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;

c) 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.

8. Dati personali particolari

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 personali genetici o dati personali biometrici intesi a identificare in modo univoco una persona fisica, dati personali relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati personali relativi a condanne penali e a reati (ex «dati personali sensibili» o «giudiziari»), il Responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

9. Documentazione e controlli

a) Le parti devono essere in grado di dimostrare il rispetto delle presenti istruzioni.

b) Il Responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del Titolare del trattamento relative al trattamento dei dati personali conformemente alle istruzioni presenti nell'atto di nomina.

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 istruzioni 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 istruzioni, 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) Qualsiasi inadempimento o violazione degli obblighi sopra stabiliti e di ogni ulteriore norma di legge applicabile, con particolare riguardo ai necessari livelli di sicurezza, anche in tema di gestione della violazione dei dati personali, ricadrà sotto l'esclusiva responsabilità del Responsabile. Ne consegue che quest'ultima risponderà in via esclusiva, tranne casi di dolo o colpa grave da parte del Titolare del trattamento nella verificazione dell'inadempimento o della violazione rilevante, di ogni richiesta di risarcimento, danno o sanzione che dovesse derivare dal mancato puntuale assolvimento dei propri obblighi.

10. Registro delle attività di trattamento

Il Responsabile del trattamento redige il Registro delle attività di trattamento ai sensi dell'art. 30, comma 2; nello specifico il Responsabile deve identificare e censire i trattamenti di dati personali, le banche dati personali e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività oggetto del contratto al fine di predisporre il registro delle attività di trattamento svolte per conto del Titolare del trattamento, da esibire, in caso di ispezione dell'Autorità di Controllo (Garante per la protezione dei dati personali).

11. Sub - Responsabili

a) Il Responsabile del trattamento può affidare a un sub-Responsabile del trattamento i trattamenti da effettuare per conto del Titolare del trattamento conformemente alle istruzioni presenti in questo atto di nomina, senza la previa autorizzazione specifica scritta del Titolare. Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base dell'elenco di cui all'allegato II. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 15 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione

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 personali imposti al Responsabile del trattamento conformemente alle presenti istruzioni. 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 istruzioni 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.

12. Trasferimento di dati personali

a) Qualunque trasferimento di dati personali 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 al punto 11 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.

13. Assistenza al Titolare del trattamento, diritti degli interessati e valutazione di impatto

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 a tali obblighi, il Responsabile del trattamento si attiene alle istruzioni del Titolare del trattamento.

c) Oltre all'obbligo di assistere il Titolare del trattamento in conformità a quanto disposto alla 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 personali e delle informazioni a disposizione del Responsabile del trattamento:

- L'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati personali») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- 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 personali indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
- 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;
- Gli obblighi di cui all'articolo 32 del 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 del presente atto di nomina, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

14. 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, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

15. Violazione riguardante dati personali trattati dal Responsabile del trattamento

a) 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, comunque entro 24 ore dal momento in cui si viene a conoscenza della violazione. La notifica contiene almeno:

- una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione);
- i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- 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.

b) 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) 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.

16. Inosservanza delle istruzioni presenti nell'atto di nomina 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 istruzioni, 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 istruzioni 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 istruzioni.

b) Il Titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti istruzioni qualora:

- 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 istruzioni non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
- il Responsabile del trattamento violi in modo sostanziale o persistente le presenti istruzioni o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
- 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 istruzioni 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 istruzioni qualora, dopo aver informato il Titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili, 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 personali non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti istruzioni.

17. Termine del trattamento

a) Il Responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato I.

b) Al termine della prestazione dei servizi relativi al trattamento il Responsabile del trattamento restituisce tutti i dati personali e cancella le copie esistenti in qualsiasi formato (elettronico, cartaceo) e su qualsiasi supporto (anche mobile o sul cloud), tranne quando diversamente richiesto da norme di legge o in ragione di prescrizioni dettate dal Garante o da altre autorità competenti.

Sede dell'impresa associata, _____

Titolare del trattamento	Responsabile del trattamento
Impresa associata	S.S.C.
_____	Giovanni Allantegana

ALLEGATO I - Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

- Lavoratori del Titolare
- Famigliari del Titolare

Categorie di dati personali trattati

Relativamente a Lavoratori del Titolare

- Dati comuni
  - dati personali identificativi
  - codice fiscale
  - dati personali di contatto (e-mail)
  - dati di accesso alla piattaforma PWS
  - dati relativi alle spese effettuate: somma senza dettagli
- dati particolari
  - dati relativi alle spese effettuate: somma senza dettagli

Relativamente a Famigliari del Titolare

- Dati comuni
  - dati personali identificativi
  - codice fiscale
  - dati relativi alle spese effettuate: somma senza dettagli
- dati particolari
  - dati relativi alle spese effettuate: somma senza dettagli

Limitazioni o garanzie applicate nel trattamento di dati particolari

- i dati di dettaglio non sono trasferiti, è conosciuta solo la somma delle spese sanitarie effettuate, senza specifiche causali
- Limitazioni all'accesso (l'accesso è consentito solo a persone autorizzate).
- Gli accessi ai dati personali sono registrati.
- Trasferimento dei dati personali solo in formato crittografato.

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

Il trattamento dei dati personali è effettuato per la gestione dei servizi di welfare aziendale: configurazione dell'accesso allapiattaforma welfare "PWS MondoWelfare", per garantire l'attuazione delle disposizioni in materia di welfare contrattuale previsti nel vigente CCRL.

Si specifica che, come riportato nel contratto firmato dalle parti all' art. 7 lett. C, l'attività di gestione della piattaforma "PWS MondoWelfare" sarà effettuata in qualità di autonomo titolare del trattamento, direttamente dalla Poste Welfare Servizi S.r.l., che riceve da parte del cliente, per il tramite di S.S.C., i dati dei lavoratori necessari all'attivazione dell'account in piattaforma e comunica al cliente (tramite S.S.C.) le Informazioni necessarie alla predisposizione della Certificazione Unica di ciascun lavoratore. Poste Welfare Servizi S.r.l. gestisce in modo totalmente autonomo la relazione con il lavoratore nell'ambito dell'utilizzo dei servizi di Welfare.
I dati trasmessi da Poste Welfare Servizi S.r.l. al cliente per il tramite di S.S.C. sono dati aggregati.

Attività svolte in qualità di Amministratori di sistema

Nella funzione di amministratore di sistema, gli operatori del Responsabile, anche per il tramite di altri Fornitori indicati in allegato II, dovranno provvedere alla configurazione della piattaforma "PWS MondoWelfare", effettuando le seguenti attività:

- Configurazione dei sistemi di accesso (autenticazione e di autorizzazione)
- Salvataggio dati (backup)

L'esecuzione di tale attività, da parte del Responsabile è finalizzata al perseguimento di un interesse esclusivo del Titolare del trattamento; i dati personali trattati dal Responsabile non saranno in alcun modo utilizzati per il perseguimento di scopi propri del Responsabile.

Natura del trattamento

Il trattamento è effettuato in modalità informatizzata e cartacea, con le misure di sicurezza individuate nell'allegato III.
Il trattamento avviene mediante le seguenti operazioni sui dati personali:

- raccolta e registrazione
- modifica/aggiornamento
- estrazione e consultazione
- comunicazione mediante trasmissione
- conservazione
- distruzione

Luogo del trattamento

I dati personali oggetto del trattamento risiedono su sistemi informatici situati:

☐ presso la sede del Titolare
☒ presso le sedi del Fornitore
☒ presso altri soggetti elencati nell'allegato II

Tutte le prestazioni oggetto del presente contratto sono erogate tramite l'utilizzo di infrastrutture interamente gestite da S.S.C. (o da Sub-fornitori) su server siti in Unione Europa.

Durata del trattamento

La presente nomina avrà la medesima durata del Contratto. Pertanto, salvo il caso in cui lo stesso non venga prorogato su intesa delle parti, le disposizioni qui stabilite cesseranno di produrre ogni effetto nel momento stesso in cui il Responsabile avrà completato l'esecuzione dei Servizi.
Per il trattamento da parte di sub- Responsabile, specificare in allegato III la materia disciplinata, la natura e la durata del Trattamento.

ALLEGATO II - Sub-Responsabili del trattamento

Il Titolare del trattamento ha autorizzato il ricorso ai seguenti sub-Responsabili del trattamento:

Sub-Responsabile	Luogo del trattamento	Descrizione del trattamento
NPO Sistemi S.r.l.	Italia	Hosting dell'infrastruttura di Confartigianato nel Data Center Aruba Servizio di backup e Disaster Recovery

ALLEGATO IIIA - <u>Misure tecniche e organizzative per garantire la sicurezza dei dati personali adottate da S.S.C.:</u>

Misure di pseudonimizzazione e cifratura dei dati personali

Misura generale	Dettaglio	Note integrative
Pseudonimizzazione dei dati personali.	In tutti i casi in cui non è necessario conoscere l'identità dell'interessato i dati devono essere trattati in modo pseudonimizzato.	NA
Cifratura dei dati personali.	Implementazione della cifratura dei dispositivi informatici utilizzati per il trattamento dei dati. I dati personali devono essere conservati in soluzioni che prevedano tecniche di cifratura. Implementazione della cifratura delle soluzioni di backup.	NA
Protezione dei dati personali fin dalla progettazione e per impostazione predefinita.	Adozione di linee guida di protezione dei dati personali fin dalla progettazione (cfr. art 25 del Regolamento), assicurandosi che i sistemi aziendali sviluppati internamente siano coerenti con esse.	

Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Misura generale	Dettaglio	Note integrative
Registrazione degli accessi	Implementazione di soluzioni di Monitoraggio degli accessi	Si
Privilegio minimo garantito	Tutti i diritti di accesso ai dati personali sono configurati con il principio di privilegio minimo (least privilege)	Si
siAggiornamenti.	Adozione di idonei mezzi tecnici e/o organizzativi in maniera tale da rendere le macchine e le applicazioni costantemente aggiornate tenendo in particolare considerazione gli aggiornamenti di sicurezza.	Si
Strumenti di protezione dei servizi e dei sistemi.	Implementazione e aggiornamento di software e hardware di protezione quali antivirus, antispam, antimalware, firewall, ecc.	Si
Isolamento sistemi non più supportati.	Segregazione fisica e/o logica delle macchine che per ragioni di operatività vengono ancora utilizzate nonostante non siano più supportate da aggiornamenti.	Si
Disponibilità dei servizi	Implementazione di misure fisiche e logiche atte a garantire la continuità del servizio (es. Sistemi ridondati, UPS, etc…)	Si
Procedure organizzative	Predisposizione ed implementazione di una procedura di emergenza	Si

Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

Misura generale	Dettaglio	Note integrative
Backup.	Implementazione di un sistema e di un piano di backup.	Si
Business Continuity Plan.	Predisposizione ed implementazione di un Business Continuity Plan. In caso di soluzione cloud valutare la Fault Tolerance della propria connettività verso i sistemi cloud.	Si
Disaster recovery.	Predisposizione ed implementazione di un piano per il Disaster Recovery, comprensivo di una procedura che definisca RTO e RPO e l'effettuazione dei relativi test periodici. In caso di soluzione cloud valutare la Fault Tolerance della propria connettività verso i sistemi cloud.	Si

Misure di identificazione e autorizzazione dell'utente

Misura generale	Dettaglio	Note integrative
Presenza di profili autorizzativi.	Definire un processo di Creazione, Gestione e Cessazione delle utenze. Creazione di profili autorizzativi da assegnare alle utenze create (alle persone autorizzate al trattamento), non assegnando più permessi del dovuto in modo da consentire la visualizzazione dei soli dati personali necessari a svolgere la funzione lavorativa assegnata. I diritti di Amministratore di sistema non devono essere assegnati agli stessi account utilizzati per effettuare le attività lavorative ordinarie. Revisione periodica dei profili di autorizzazione, almeno annuale.	Si
Credenziali individuali.	Creazione di credenziali individuali per ciascun incaricato e implementazione di un sistema di gestione delle password con particolare riferimento a complessità. Non deve essere possibile accedere ai dati con credenziali non individuali. Prevedere scadenza rafforzata della password nel caso non sia presente il secondo fattore di autenticazione.	Si
Rate limiting.	Impostazione di un numero massimo di tentativi falliti di login prima del blocco dell'account su tutti i sistemi e applicativi aziendali.	Si
Network Access Control.	Introduzione di una soluzione per autenticare le macchine sulla rete, nel caso di infrastruttura locale.	Si
Protezione delle credenziali.	I sistemi devono garantire l'impossibilità di risalire alla password degli utenti Le password degli utenti sono crittografate	Si
Protezione delle sessioni.	Implementazione di un sistema di blocco schermo con reinserimento della password ogni qualvolta non vi è fisicamente un incaricato presente a presidiare/utilizzare la postazione di lavoro.	Si

Misure di protezione dei dati personali durante la trasmissione

Misura generale	Dettaglio	Note integrative
Protezione dei dati personali durante la trasmissione.	Implementazione di protocolli di sicurezza che proteggano i dati in tutte le comunicazioni in cui è previsto il trattamento di dati personali (es: https, sftp, TLS, VPN…).	Si

Amministratori di Sistema, misure da attuare in funzione della qualifica di Amministratore di sistema

Misura generale	Dettaglio	Note integrative
Attuazione delle misure prescritte dal Garante per la protezione dei dati personali in merito all'attribuzione delle funzioni di "**Amministratore di Sistema**" di cui al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008.	Designare come Amministratore di Sistema, con le modalità previste dal provvedimento del 27 novembre 2008, le persone fisiche autorizzate ad accedere in modo privilegiato (ai sensi dello stesso provvedimento) ai dati personali oggetto del trattamento; Conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte all'interno della struttura organizzativa del Responsabile del trattamento quali Amministratori di Sistema (in relazione ai dati personali oggetto del trattamento); Implementare un sistema idoneo alla registrazione degli accessi logici degli Amministratori di Sistema conforme al Provvedimento menzionato; Effettuare la verifica, con cadenza almeno annuale, sull'operato degli Amministratori di Sistema secondo quanto prescritto dallo stesso provvedimento; gli esiti di tali verifiche dovranno essere comunicati al Titolare del trattamento su richiesta dello stesso.	Si

Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

Misura generale	Dettaglio	Note integrative
Sicurezza Fisica.	Implementare misure tecniche e organizzative per consentire l'accesso fisico agli uffici solo al personale autorizzato ed istruito. Implementare misure tecniche e organizzative per consentire l'accesso fisico a uffici tecnici solo al personale autorizzato ed istruito. Implementare misure tecniche e organizzative per garantire la sicurezza fisica degli uffici tecnici o apparati di rete, quali Antintrusione Previsione di procedure sicure per la custodia dei supporti di backup.	Si

Misure di protezione dei dati personali trattati su supporti cartacei

Misura generale	Dettaglio	Note integrative
Protezione supporti cartacei.	Archiviazione di documenti cartacei contenenti dati personali in armadi chiusi Implementare misure tecniche e organizzative per consentire l'accesso fisico ai luoghi di conservazione dei documenti cartacei contenenti dati personali solo al personale autorizzato ed istruito.	Si

Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento

Misura generale	Dettaglio	Note integrative
Piani di ripristino.	Implementazione di procedure di ripristino ed effettuazione dei relativi test periodici.	Si
Vulnerability Assessment	Realizzazione di vulnerability assessment sull'infrastruttura.	Si
Penetration testing	Realizzazione di penetration testing sui dispositivi usati per il trattamento dei dati personali. Realizzazione di penetration testing sull'infrastruttura. Realizzazione di penetration testing sugli apparati di rete	NO
Security Operation Center	Implementazione di sistemi in grado di rilevare e gestire in tempo reale anomalie che possono verificarsi nei flussi di dati	Si

Formazione

Misura generale	Dettaglio	Note integrative
Formazione.	Effettuare sensibilizzazione periodica sulle **minacce informatiche** e sull'adozione di comportamenti corretti per tutto il personale coinvolto nel trattamento. Formazione normativa sul trattamento dei dati	Si

Gestione degli incidenti e delle violazioni

Misura generale	Dettaglio	Note integrative
Procedure di gestione degli incidenti.	Definizione di una procedura per la gestione degli incidenti, tale da gestire tutti gli incidenti di sicurezza che possono coinvolgere dati personali, definendo ruoli e responsabilità	Si
Formazione del personale.	Definire un piano di formazione del personale sulle procedure di gestione degli incidenti.	Si
Registro degli incidenti.	Mantenere un registro degli incidenti, che contenga almeno le informazioni in merito a scoperta, analisi, contenimento, mitigazione e recupero dai vari incidenti di sicurezza.	Si
Comunicazione al Titolare.	Comunicare tempestivamente al Titolare, nell'arco di 24 ore dalla scoperta, gli incidenti di sicurezza occorsi sulle loro infrastrutture.	Si

Supporto al Titolare per la gestione delle richieste degli interessati

Assistere e supportare il Titolare del trattamento fornendo tempestivamente tutte le informazioni necessarie e/o i documenti utili al fine di soddisfare l'obbligo del Titolare del trattamento di dare riscontro alle richieste per l'esercizio dei diritti dell'interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile) nel rispetto dei termini di cui al Capo III del Regolamento (ad es.: esercizio dei diritti di accesso, rettifica, limitazione, opposizione al trattamento dei dati personali).

Misure di certificazione/garanzia di processi e prodotti

(Completare se il Responsabile adotta sistemi di gestione certificato, per es. 9001, 27001, etc. Altrimenti indicare NA)

☐ Non applicabile

☒ Applicabile, si adottano i seguenti sistemi di certificazione

- ISO 9001:2025