

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI A NORMA DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, DEL 27 APRILE 2016, RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI (GENERAL DATA PROTECTION REGULATION – “GDPR”) - CLAUSOLE CONTRATTUALI TIPO

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

- Scopo delle presenti clausole contrattuali tipo (le “**Clausole**”) è garantire il rispetto dell'art. 28, parr. 3 e 4, del GDPR.
- I titolari del trattamento e i responsabili del trattamento di cui all'allegato I accettano queste Clausole per garantire il rispetto dell'art. 28, parr. 3 e 4, del GDPR.
- Queste Clausole si applicano al trattamento dei dati personali specificato all'allegato II.
- Gli allegati da I a IV costituiscono parte integrante delle Clausole.
- Le presenti Clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del GDPR.
- Le presenti Clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del GDPR.

Clausola 2

Invariabilità delle Clausole

- Le parti s'impegnano a non modificare le Clausole se non per aggiungere o aggiornare informazioni negli allegati.
- Ciò non impedisce alle parti d'includere le presenti Clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti Clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3

Interpretazione

- Quando le presenti Clausole utilizzano i termini definiti nel GDPR, tali termini hanno lo stesso significato di cui al GDPR.
- Le presenti Clausole vanno lette e interpretate alla luce delle disposizioni del GDPR.
- Le presenti Clausole non vanno interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal GDPR o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4

Gerarchia

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

Clausola 5

Clausola di adesione successiva

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

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6

Descrizione del trattamento

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

Clausola 7

Obblighi delle parti

7.1. Istruzioni

- Il responsabile del trattamento tratta i dati personali solo 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 tale 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 GDPR o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

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

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali solo per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

- Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
- Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

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

7.6 Documentazione e rispetto

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

7.7. Ricorso a sub-responsabili del trattamento

- a. Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. 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 20 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. Ove il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti Clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti Clausole e del GDPR.
- 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 d'imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

- a. Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del GDPR.
- b. Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla Clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del GDPR, il responsabile del trattamento e il

sub-responsabile del trattamento possono garantire il rispetto del capo V del GDPR utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del GDPR, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8

Assistenza al titolare del trattamento

- a. Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tale senso dal titolare del trattamento.
- b. Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.
- c. Oltre all'obbligo di assistere il titolare del trattamento in conformità della Clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:
 1. l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (data protection impact assessment – "DPIA") qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
 2. l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
 3. l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
 4. gli obblighi di cui all'art. 32 GDPR.
- d. Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente Clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9

Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli artt. 33 e 34 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

- a. nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso e a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
- b. nell'ottenere le seguenti informazioni che, in conformità all'art. 33, par. 3 del GDPR, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
 1. la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo d'interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 2. le probabili conseguenze della violazione dei dati personali;
 3. le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

- c. nell'adempiere, in conformità dell'art. 34 GDPR, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

- a. una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo d'interessati e di registrazioni dei dati in questione);
- b. i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- c. le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli artt. 33 e 34 del GDPR.

SEZIONE 6 - DISPOSIZIONI FINALI

Clausola 10

Inosservanza delle Clausole e risoluzione

- a. Fatte salve le disposizioni del GDPR, ove il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti Clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti Clausole o non sia risolto

il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti Clausole.

- b. Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti Clausole ove:
 1. il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti Clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
 2. il responsabile del trattamento violi in modo sostanziale o persistente le presenti Clausole o gli obblighi che gli incombono a norma del GDPR;
 3. il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti Clausole o del GDPR.
- c. Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti Clausole ove, dopo avere informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della Clausola 7.1, lett. b), il titolare del trattamento insista sul rispetto delle istruzioni.
- d. Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti Clausole.

ALLEGATO I - ELENCO DELLE PARTI

1. Nome:

Indirizzo:

Nome, qualifica e dati di contatto del referente:

Nome e dati di contatto del responsabile della protezione dei dati:

Ruolo nel trattamento dei dati personali:

Titolare del trattamento

Responsabile del trattamento

Firma e data di adesione:

2. Nome: *Poste Italiane S.p.A.*

Indirizzo: *Viale Europa, 190 – 00144 Roma*

Nome, qualifica e dati di contatto del referente:

Nome e dati di contatto del responsabile della protezione dei dati: *Francesco Tavone - Ufficio del Responsabile della Protezione dei Dati di Poste Italiane, viale Europa, 175 (00144) Roma - e-mail: ufficiorpd@posteitaliane.it*

Ruolo nel trattamento dei dati personali:

Titolare del trattamento

Responsabile del trattamento

Firma e data di adesione:

ALLEGATO II: DESCRIZIONE DEL TRATTAMENTO

Categorie di interessati i cui dati personali sono trattati

Cittadini residenti nel territorio di

Categorie di dati personali trattati: Dati comuni

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi

☒ NO ☐ SI

Natura del trattamento

Il trattamento è connesso all'esecuzione del servizio oggetto dell'accordo principale cui le presenti Clausole accedono.

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

Svolgimento di campagne di rilevazione, mediante la somministrazione di un breve questionario rivolto a fasce specifiche di popolazione, allo scopo di:

- acquisire informazioni relative all'interesse e alla fornitura di servizi welfare offerti dalle amministrazioni locali;
- comunicare iniziative specifiche;
- individuare bisogni e acquisire richieste di contatto utili all'attivazione di servizi dedicati;
- supportare le persone anziane nella comunicazione e attivazione di servizi digitali;
- Supportare le amministrazioni nell'aggiornamento dei piani protezione civile.

Durata del trattamento

Il trattamento avrà la medesima durata dell'accordo principale cui le presenti Clausole accedono.

Per il trattamento da parte di sub-responsabili del trattamento, materia disciplinata, natura e durata del trattamento

[Vedi Allegato IV del presente contratto]

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

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

- MT01 Il fornitore deve adottare regole per controllare l'accesso fisico e logico alle informazioni, ai dati personali e alle altre risorse associate in base ai requisiti di sicurezza delle informazioni e dei dati personali trattati.
- MT02 Il fornitore deve garantire l'identificazione univoca degli individui e dei sistemi che accedono alle informazioni, ai dati personali e alle risorse associate, nonché garantire un'adeguata assegnazione dei diritti di accesso. Il fornitore, inoltre, deve garantire la gestione di eventuali modifiche alle informazioni correlate all'identità degli utenti.
- MT03 Il fornitore garantisce il controllo dell'assegnazione e della gestione delle informazioni di autenticazione, inclusa la formazione del personale sul trattamento appropriato delle credenziali di autenticazione.
- MT05 Le password devono essere sostituite almeno ogni 6 mesi.
- MT07 I diritti di accesso alle informazioni, ai dati personali e alle altre risorse associate devono essere forniti sulla base di criteri di necessità, rivisti periodicamente e, se necessario, prontamente modificati e rimossi dal fornitore.
- MT10 Il fornitore riduce al minimo il numero di soggetti con diritti di accesso privilegiato o di livello amministratore.
- MT11 Il fornitore garantisce la registrazione degli eventi (log), anche al fine di generare prove, garantire l'integrità delle informazioni e dei dati personali, prevenire accessi non autorizzati e identificare eventi di sicurezza.
- MT12 Il fornitore garantisce una sicura e corretta configurazione e gestione dei dispositivi endpoint degli utenti.
- MT13 Il fornitore adotta tecniche di autenticazione adeguate per comprovare l'identità di utenti, software, messaggi e altre entità. La forza dell'autenticazione deve essere adeguata alla classificazione delle informazioni e dai dati personali trattati. Laddove è richiesta un'autenticazione forte e una verifica dell'identità, sono utilizzati metodi di autenticazione alternativi alla password.
- MT14 Il fornitore garantisce la cancellazione delle informazioni e dei dati personali archiviati nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione quando non più necessari, utilizzando sistemi di cancellazione sicuri ed approvati, per eliminare in modo permanente le informazioni e i dati personali e per garantire che questi non possano essere recuperati utilizzando strumenti di recupero specialistici.
- MT15 Il fornitore corregge prontamente le vulnerabilità tecniche dei sistemi informativi in uso, valutando l'esposizione a tali vulnerabilità e adottando misure appropriate.
- MT17 Il fornitore monitora l'utilizzo delle risorse per garantire e, ove necessario, migliorare la disponibilità e l'efficienza dei sistemi.
- MT18 Il fornitore pianifica ed è preparato per la gestione degli incidenti legati alla sicurezza delle informazioni e dei dati personali. Stabilisce le responsabilità, comunica ruoli e processi di gestione degli incidenti di sicurezza, al fine di garantire una risposta rapida, efficace, coerente e ordinata agli incidenti relativi alla sicurezza delle informazioni e dei dati personali.
- MT19 Il fornitore definisce e applica norme per lo sviluppo sicuro di software e sistemi, tenendo in considerazione misure quali, ad esempio, la separazione degli ambienti di sviluppo, test e produzione.
- MT20 Il fornitore garantisce che le copie di backup di informazioni e dati personali, software e sistemi siano mantenute e regolarmente testate, per consentire il pronto ripristino e evitare la perdita di dati.
- MT21 Il fornitore ricorre a tecniche di mascheramento, pseudonimizzazione, anonimizzazione e crittografia dei dati per limitare l'esposizione di dati personali nonché qualora richiesto da requisiti normativi e contrattuali.
- MT23 Il fornitore adotta misure opportune per la gestione sicura dei supporti di memorizzazione rimovibili. In particolare, se i supporti di memorizzazione contengono informazioni riservate e dati personali devono essere riutilizzati, vengono adottate procedure di cancellazione sicura dei dati prima del loro riutilizzo. Inoltre, i supporti di memorizzazione, quando non più necessari, sono smaltiti in modo sicuro.
- MT24 Il fornitore, qualora venga a conoscenza di una eventuale violazione di dati personali, informa tempestivamente il titolare, in modo che possa attivarsi, ai sensi dell'art. 33 GDPR.
- MT25 Il fornitore adotta le misure e gli accorgimenti prescritti in materia di attribuzioni delle funzioni di amministratore di sistema (Provvedimento del 27 novembre 2008 27 novembre 2008, modificato dal Provvedimento del 25 giugno 2009).
- MT26 Il fornitore garantisce il rispetto dei diritti riconosciuti ai soggetti interessati, di cui agli artt. 15-22 GDPR.

- CSP01 La Società utilizza Data Center ubicati esclusivamente all'interno dell'UE sia per l'erogazione dei servizi che per il backup e il disaster recovery.
- CSP02 La Società deve permettere attività di audit da parte di Poste Italiane o suoi incaricati nelle modalità concordate contrattualmente o secondo esigenze (ad es. incidenti di sicurezza).
- CSP03 La Società garantisce canali sicuri di trasmissione dati tra i Data Center e Poste Italiane.
- CSP04 La Società garantisce la possibilità di attivare un livello di crittografia dei dati tramite chiave crittografica gestita direttamente da Poste Italiane (BYOK), in caso di fornitura di servizi IaaS e PaaS.
- CSP05 La Società garantisce la restituzione e la cancellazione sicura dei dati da supporti fisici e buffer di memoria alla fine della fornitura/contratto.
- CSP06 La Società garantisce l'adozione di misure atte a mitigare gli effetti di attacchi di tipo denial of service (DoS/DDoS), sia dall'esterno sia dall'interno.
- CSP07 La Società garantisce la registrazione di tutti i log relativi agli accessi e alle operazioni effettuate da utenze amministrative, ad elevati privilegi e applicative.
- CSP08 La Società garantisce la possibilità di attivare il tracciamento delle operazioni svolte dagli utenti (interni ed esterni) a fronte di esigenze normative applicabili a Poste Italiane.
- CSP09 La Società in caso di trattamento di dati personali in paesi extra UE garantisce la sottoscrizione delle Standard Contractual Clauses (SCC) nell'ultima versione pubblicata dalla Comunità Europea o, in sub-ordine, delle Binding Corporate Rules e di ulteriori misure di sicurezza che dovranno essere condivise/modificate su richiesta.
- CSP10 Il requisito è esteso anche agli eventuali sub-fornitori cui la Società intenda avvalersi.
- CSP11 La Società ha predisposto un Transfer Impact Assessment (TIA) per ogni trattamento di dati personali svolto in paesi extra UE e lo mette a disposizione su richiesta.

Descrizione delle misure tecniche e organizzative specifiche che il/i sub-responsabile/i del trattamento deve/ono prendere per essere in grado di fornire assistenza al titolare del trattamento.

Gli eventuali sub-responsabili del trattamento devono adottare le medesime misure tecniche e organizzative di cui al punto precedente, nella misura in cui rilevino con riguardo al trattamento loro affidato.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

- MO01 Il fornitore ha definito policy e procedure per la gestione dei terzi che trattano dati personali (nomina a responsabile del trattamento, contratti con i fornitori, SLA, ecc.).
- MO02 Il fornitore ha definito una policy per la classificazione del livello di riservatezza dei dati (dati pubblici, per uso interno, confidenziali/riservati, ecc.).
- MO03 Il fornitore gestisce correttamente l'archiviazione cartacea dei dati e, a tal fine, ha definito policy e procedure per la gestione di archivi cartacei contenenti dati personali.
- MO04 Il fornitore ha definito policy e procedure per la gestione del rischio privacy (Data Privacy Impact Assessment).
- MO05 Il fornitore ha definito policy e procedure per la gestione degli accessi logici, includendo, a titolo esemplificativo ma non esaustivo, aspetti relativi all'identificazione e all'abilitazione degli utenti, alla complessità delle password, ecc.
- MO06 Il fornitore ha definito policy per la gestione degli accessi fisici.
- MO07 Il fornitore ha definito una procedura per la gestione dei data breach.
- MO08 Il fornitore ha definito policy e procedure per garantire l'esercizio dei diritti degli interessati.
- MO09 Il fornitore coopera, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.

Istruzioni in caso di Data Breach o presunta violazione di dati personali: elementi che il Responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

Nei casi in cui il Responsabile rilevi una presunta violazione dei dati personali deve essere avviata tempestivamente l'analisi del caso.

A tal fine, il referente del Responsabile notifica al Titolare del trattamento e al RPD dello stesso che è in corso la valutazione di un incidente di sicurezza fornendo, altresì, una prima sommaria descrizione dell'incidente e assegnando un identificativo univoco allo stesso.

Nel caso in cui sia il Titolare a venire a conoscenza di un incidente di sicurezza caratterizzato da una possibile violazione dei dati personali (data breach) che necessita dell'intervento tecnico del Responsabile, il Titolare informa il referente contrattuale del Responsabile (cfr. riferimenti dell'allegato I) che coinvolge tempestivamente il proprio RPD.

Le competenti strutture del Responsabile avviano le pertinenti verifiche, al termine delle quali forniscono al Titolare tutte le informazioni necessarie ai fini della valutazione dell'eventuale violazione, assegnando un identificativo unico all'incidente stesso.

La comunicazione deve contenere le seguenti informazioni:

- tipologia dell'incidente;
- descrizione del servizio impattato e/o della banca dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- circostanze dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuare possibili effetti negativi;
- proposta di comunicazione di violazione di dati personali al/agli interessato/i in base ad un'analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, comma 3, del GDPR, che escludono la necessità di comunicazione della violazione all'interessato.

Il Titolare valuta la segnalazione e la completezza delle informazioni ed eventualmente richiede ulteriori informazioni nel caso in cui la ritenesse non esaustiva.

ALLEGATO IV: ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

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

1. Nome: Microsoft Ireland Operations Limited Ltd
Indirizzo: One Microsoft Place South Country Business Park – Dublino – Irlanda
Nome, qualifica e dati di contatto del referente: Marcin Rucinski
Descrizione del trattamento: per tutte le modalità di trattamento dei dati si rimanda al documento “Microsoft Products and Services Data Protection Addendum (DPA)”
Categorie di interessati i cui dati personali sono trattati:
 - Mittenti e destinatari delle spedizioni
 - Categorie di dati personali trattati:
 - Dati anagrafici
 - Dati di contatto
 - Dati di geolocalizzazione delle spedizioni
2. Nome: Avanade Italy S.r.l
Indirizzo: Via Del Mulino n° 11/A - 20057 Assago
Nome, qualifica e dati di contatto del referente: Emiliano Rantucci, Via Del Mulino n° 11/A - 20057 Assago (MI), tel 02/760491 - avanadeitaly@legalmail.it
Descrizione del trattamento
Categorie di interessati i cui dati personali sono trattati:
 - Mittenti e destinatari delle spedizioni
 - Categorie di dati personali trattati:
 - Dati anagrafici
 - Dati di contatto
 - Dati di geolocalizzazione delle spedizioni