PREMESSO

- che in data odierna (o indicare altra data precedente), per il Servizio di ……
(indicare brevemente il servizio affidato: es. servizio di videosorveglianza, servizio di assistenza domiciliare, servizio gestione sito web, ecc.)……, tra Azienda sanitaria locale TO4 di Ciriè, Chivasso e Ivrea e Società/Associazione/Professionista …… (di seguito anche "Parti"), è stipulato Contratto/Convenzione/Concessione/…, il cui contenuto si intende integralmente riportato e trascritto nel presente atto, e che in tale servizio rientrano attività che comportano o possono comportare un trattamento di dati personali;
- Azienda sanitaria locale TO4 di Ciriè, Chivasso e Ivrea, in qualità di titolare del trattamento dei dati personali ("titolare") ai sensi dell'art. 4, punto 7, GDPR, ritiene che Società/Associazione/Professionista……, nell'ambito delle attività/prestazioni professionali e dei servizi affidati, di cui al contratto richiamato, abbia i requisiti di esperienza, capacità ed affidabilità tali da fornire idonea garanzia del pieno rispetto delle disposizioni stabilite nel GDPR e nel D.lgs. 196/2003 s.m.i., ivi compresa la capacità di mettere in atto misure di sicurezza tecniche ed organizzative adeguate;
- Società/Associazione/Professionista……, in qualità di responsabile del trattamento dei dati personali ("responsabile") è tenuta, pertanto, a comunicare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico;

con il presente atto, le Parti, al fine di disciplinare i trattamenti di dati personali rientranti nelle attività richiamate, convengono quanto segue

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

a) Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

g) Il responsabile non ha diritto ad alcun compenso specifico ulteriore per l'esecuzione delle attività descritte nel presente atto, in quanto svolte nell'ambito dell'incarico in essere, per il quale è stata già definita l'intera valutazione economica del rapporto contrattuale.

Clausola 2 - Invariabilità delle clausole

a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

a) Quando le presenti clausole utilizzano i termini definiti, rispettivamente, nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.

b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

a) 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

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

a) 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.

b) Per ciascun trattamento di propria competenza, il responsabile deve fare in modo che siano sempre rispettati i principi applicabili al trattamento dei dati personali[1].

c) Il responsabile si impegna a mantenere i requisiti di esperienza, capacità e affidabilità.

d) Il responsabile deve tenere conto che il trattamento è lecito solo se e nella misura in cui venga rispettata la base giuridica individuata ai sensi dell'art. 6, GDPR.

Clausola 7 - Obblighi delle parti

Obblighi del responsabile del trattamento

7.1. Istruzioni

a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

[1] Art. 5, GDPR: «i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità; i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare e rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali».

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

7.3. Durata del trattamento dei dati personali

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

7.4. Sicurezza del trattamento

a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative[2] specificate nell'allegato III per garantire la sicurezza dei dati personali. Tali misure devono essere periodicamente aggiornate sulla base del progresso tecnologico. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b) Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza, il responsabile si impegna a comunicarlo per iscritto al titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate.

c) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale (soggetti "autorizzati" o "designati") 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. Il responsabile è, altresì, tenuto, nella propria organizzazione, a formare le persone autorizzate al trattamento per i dati affidati e fornire loro le istruzioni adeguate, attuando un controllo sulla loro attività svolta al fine di verificare l'effettivo rispetto delle misure di sicurezza adottate e, comunque, delle istruzioni impartite. Il responsabile è tenuto, altresì, ad assegnare agli autorizzati del trattamento, a seconda dei compiti attribuiti ad ognuno e laddove sia tecnicamente possibile, le credenziali di autenticazione che permettano di svolgere solo le operazioni di propria competenza, nonché le dovute responsabilità per le aree ad accesso controllato, ove presenti.

7.5. Dati sensibili ("categorie particolari di dati" ai sensi degli articoli 9 e 10, GDPR)

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

7.6. Documentazione e rispetto

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

b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

---

[2] Art. 32, GDPR: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati».

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. Le risultanze dell'audit saranno discusse in buona fede tra le Parti e il responsabile si impegna sin d'ora ad attuare gli eventuali cambiamenti ritenuti necessari dal Titolare in seguito all'audit, al fine di garantire la conformità alla normativa vigente e alle norme contrattuali.

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[3]

a) **AUTORIZZAZIONE PRELIMINARE SPECIFICA**: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno 15 giorni prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679, svolgendo un'accurata due diligence volta ad assicurarsi che il Sub-Responsabile del trattamento sia in grado di garantire un adeguato livello di protezione dei dati personali e abbia adeguata esperienza, capacità e affidabilità.

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.

f) Qualora il responsabile ritenga di non essere in grado di eseguire le prestazioni di cui al Contratto senza l'apporto di un sub- responsabile del Trattamento, il titolare avrà diritto di risolvere il Contratto, ed il presente atto, ai sensi e per gli effetti di cui all'art. 1456 c.c.

7.8. Trasferimenti internazionali

---

[3] Art. 28, par. 2, GDPR: «Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche».

Art. 28, par. 4, GDPR: «Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile».

a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

7.9 Registro dei trattamenti

a) Il responsabile, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante *ratione materiae*, deve redigere il registro dei trattamenti svolti, come previsto dall'art. 30, GDPR, e fornire al titolare un estratto della predetta mappatura riveniente nel trattamento scaturente dal presente atto.

7.10 Informativa

a) Ogni qualvolta si raccolgano direttamente dati personali, il responsabile provvede a che venga fornita l'informativa ai soggetti interessati, ai sensi degli articoli 13 e 14, GDPR.

7.11 Nomina del responsabile della Protezione dei Dati Personali (DPO)

a) Il responsabile è tenuto a provvedere, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante *ratione materiae*, alla nomina di un proprio responsabile della Protezione dei Dati personali (DPO)[4], quale figura di raccordo per le questioni attinenti alla protezione dei dati personali con il titolare e comunicare il nominativo e i dati di contatto del responsabile della Protezione dei Dati personali al titolare.

7.12 Nomina e comunicazione degli Amministratori di sistema

a) Il titolare, ove ne ricorrano i presupposti previsti dalla normativa in materia di protezione dei dati personali e dai Provvedimenti del Garante ratione materiae, attribuisce al responsabile il compito di dare attuazione alle prescrizioni di cui al Provvedimento generale del Garante privacy del 27 novembre 2008 e s.m.i., relativo alle "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".

b) Il responsabile, lì dove ne ricorrano i presupposti stabiliti dalla normativa vigente in materia di protezione dati, dovrà dunque:

- procedere alla designazione individuale degli Amministratori di Sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;
- dare comunicazione al titolare della/e nomina/e ad Amministratore di Sistema, specificando la/le persona/e nominata/e in tale veste, riportando per ciascun Amministratore di Sistema designato, o figura equivalente, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, nonché i dati di contatto dello/degli stesso/i;
- comunicare la nomina ad Amministratore di Sistema all'organizzazione aziendale e al personale interessato con le modalità più opportune (ad es. mediante specifico ordine di servizio);
- nel caso di servizi di Amministrazione di Sistema affidati in outsourcing ad un sub-responsabile, il responsabile deve conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratore di Sistema, nonché fornire al titolare tutte le indicazioni di cui ai punti che precedono;
- conservare in ogni caso gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema o figura equivalente;

[4] Artt. 37-39, GDPR.

- verificare, con cadenza almeno annuale, l'operato degli Amministratori di sistema o figure equivalenti in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza per il trattamento dei dati personali previste dalle norme vigenti e predisporre con cadenza trimestrale (o altra cadenza) una relazione scritta delle attività svolte in esecuzione degli incarichi assegnati in forza del presente atto.
- adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema o figure equivalenti; le registrazioni dovranno essere conservate per un congruo periodo, comunque non inferiore a sei mesi.
- assicurarsi della qualità delle copie di back up e della loro conservazione in luogo sicuro e adatto, nonché della custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

Obblighi del titolare

7.13 Scopi del titolare

a) Il titolare del trattamento persegue le seguenti finalità:

● Conformità: il titolare è responsabile per la valutazione della legittimità del trattamento dei dati e nel garantire i diritti degli interessati coinvolti;

● Sicurezza: le misure tecniche e organizzative adottate devono garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e dalla natura dei dati da proteggere, tenendo conto dello stato dell'arte e del costo della loro attuazione; il titolare riesce a dimostrare che il trattamento è effettuato conformemente a quanto previsto dal Regolamento (UE) 2016/679;

● Istruzioni: il titolare rilascerà istruzioni scritte riguardanti lo scopo e la procedura del trattamento dei dati, se del caso, amplificando, specificando e modificando le clausole di questo atto; le istruzioni orali saranno immediatamente confermate per iscritto e saranno parte integrante e sostanziale delle presenti clausole.

7.14 Competenza del titolare

a) Il presente accordo lascia impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del GDPR. Il titolare è competente per il rispetto dei principi di liceità e correttezza del trattamento di cui all'art. 5, GDPR, e deve essere in grado di dimostrare che il trattamento è effettuato conformemente alla normativa nazionale ed europea in materia di protezione dei dati personali. Segnatamente, restano di competenza del titolare tutte le valutazioni in ordine alla liceità del trattamento affidato al responsabile ed ogni ulteriore adempimento previsto dalla normativa in materia di protezione dei dati personali, quali in via meramente esemplificativa: informazioni da rendere agli interessati ex artt. 13 e 14, GDPR, lo svolgimento delle valutazioni di impatto sulla protezione dei dati e la raccolta, gestione e conservazione del consenso ex art. 7, GDPR, ove necessario. Parimenti resta di competenza del responsabile l'adozione, con riferimento alla propria organizzazione interna, di tutte le necessarie misure di sicurezza tecniche ed organizzative anche in conformità alla disciplina in materia di Amministratori di Sistema.

Clausola 8 - Assistenza al titolare del trattamento

a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, ai sensi degli artt. 15-22, GDPR[5], 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) Il responsabile del trattamento assiste il titolare del trattamento al fine di eseguire eventuali indicazioni o ordini emessi dall'Autorità di Controllo o dalle Autorità Giudiziarie in relazione al trattamento dei dati, e per evadere tempestivamente e adeguatamente le richieste del titolare in ordine alle indicazioni e alle linee guida dell'Autorità di Controllo in materia di protezione dei dati personali, essendo, altresì, tenuto ad informare tempestivamente il

[5] Art. 15 "Diritto di accesso dell'interessato", art. 16 "Diritto di rettifica", art. 17 "Diritto alla cancellazione («diritto all'oblio»), art. 18 "Diritto di limitazione di trattamento", art. 19 "Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento", art. 20 "Diritto alla portabilità dei dati", art. 21 "Diritto di opposizione", art. 22 "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione".

titolare in merito ad ispezioni eseguite da parte del Garante privacy o dell'Autorità Giudiziaria con riferimento ai Trattamenti dei dati personali.

d) Il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

e) Per eventuali richieste del responsabile della Protezione dei Dati Personali (DPO) nominato dal titolare, nell'esecuzione dei suoi compiti.

f) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679[6], tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1. Violazione riguardante dati trattati dal titolare del trattamento

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

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

2) le probabili conseguenze della violazione dei dati personali;

3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

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

[6] Art. 33, GDPR: «1.In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2.Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione».
Art. 34, GDPR: «1.Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo».

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2. Violazione riguardante dati trattati dal responsabile del trattamento

a) In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento entro 24 ore (e comunque senza ingiustificato ritardo, anche se durante le festività) dopo esserne venuto a conoscenza, mediante la compilazione del modulo ad hoc (Allegato V), restando a piena disposizione del titolare, in particolare collaborando attivamente con il medesimo nella raccolta documentale e in tutte le attività, anche di indagine, connesse alla valutazione e all'effettuazione dell'eventuale notifica al Garante privacy e ai soggetti interessati, ai sensi degli artt. 33 e 34, GDPR.

b) Qualora il responsabile non comunichi al titolare entro 24 ore l'avvenuta violazione dei dati, è tenuto a motivare tale ritardo.

c) 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.

SEZIONE III - DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

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

- 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;
- il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
- il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.

c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Alla cessazione o risoluzione del contratto, il responsabile del trattamento:

- restituisce entro 30 giorni le relative copie oggetto del trattamento e ogni altra informazione, di proprietà del titolare e rilevanti sotto il profilo della protezione dei dati personali, in un formato comune, leggibile, tale da poter tener conto del progresso tecnologico, favorendo la consultazione e il riutilizzo dei dati in capo al titolare;
- a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali, cancella tutti i dati personali trattati per conto del titolare e certifica a quest'ultimo di averlo fatto.

e) Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

Clausola 11 – Legge applicabile e foro competente

a) Il presente atto, salvo quanto diversamente ivi previsto, in linea con il GDPR, è regolato dalle leggi della giurisdizione del titolare.

b) La sede esclusiva per tutte le controversie derivanti da o in connessione con questo atto di nomina è il luogo di stabilimento del titolare, fatto salvo il diritto di quest'ultimo di presentare un'azione giudiziaria contro il responsabile, di fronte a qualsiasi altro tribunale ritenuto competente.

ALLEGATO I - Elenco delle parti

I.1 Titolare del trattamento:

Nome o ragione sociale: Azienda sanitaria locale TO4 di Ciriè, Chivasso e Ivrea

Indirizzo: ……

Nome, qualifica e dati di contatto del referente: ……

Firma e data di adesione: ……

*(qualora a firmare il documento sia persona fisica diversa dal rappresentante legale del Titolare, indicare nome, cognome e qualifica della medesima persona, ad esempio DOTT. MARIO ROSSI, DIRIGENTE DELL'UFFICIO GARE dell'*Azienda sanitaria locale TO4 di Ciriè, Chivasso e Ivrea)

Responsabile protezione dei dati (DPO) del titolare del trattamento:

Cap&G Consulting srl, Via Cerreto, 37 82035 San Salvatore Telesino (BN), info@capg.it, +39 0824 041242

I.2 Responsabile del trattamento

Nome o ragione sociale: ……

Indirizzo: ……

Nome, qualifica e dati di contatto del referente: ……

Firma e data di adesione: ……

(qualora a firmare il documento sia persona fisica diversa dal responsabile, indicare nome, cognome e qualifica della medesima persona, ad esempio ING. PAOLO VERDI, RESPONSABILE AREA CONTRATTI DELLA SOCIETA' ALPHA SRL oppure RAPPRESENTANTE LEGALE DELLA SOCIETA' ALPHA SRL)

Responsabile protezione dei dati (DPO) del responsabile del trattamento:

(nome, cognome, indirizzo e-mail)

……

ALLEGATO II - Descrizione del trattamento

II.1 Categorie di interessati i cui dati personali sono trattati

……

…… *(INDICARE ad es. minori casa - famiglia, dipendenti comunale, assistiti a domicilio, utenti del sito web, ecc.)*……

II.2 Categorie di dati personali trattati

a) □ Dati comuni

……..(*INDICARE ad es.: nome, cognome, codice fiscale, e-mail, residenza, ISEE, ecc.*)……

b) □ 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

……(*INDICARE ad es.: patologia, situazione di disagio economico, credo religioso, origine razziale, sindacato, orientamento sessuale, ecc.*)……

c) □ Dati relativi a condanne penali e a reati

……..(*INDICARE ad es.: certificato del casellario giudiziale, ecc.*)……

II.3 Se sono state barrate le caselle relative alle lettere b) e/o c) indicare le limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

COME DA ALLEGATO III

II.4 Natura del trattamento

Le attività di trattamento consistono nelle operazioni di:

(BARRARE CASELLE CORRISPONDENTI ALLE OPERAZIONI DI TRATTAMENTO EFFETTUATE DAL RESPONSABILE DEL TRATTAMENTO)

□ raccolta □ registrazione □ organizzazione □ strutturazione

□ conservazione □ adattamento o modifica □ estrazione □ consultazione

□ uso □ comunicazione mediante trasmissione (ad es. a soggetti pubblici che ne facciano richiesta per il proseguimento dei propri fini istituzionali e se prescritto dalla normativa vigente comunitaria e nazionale) □ diffusione o qualsiasi altra forma di messa a disposizione □ raffronto o interconnessione □ limitazione □ cancellazione o distruzione □ elaborazione ed uso per fini statistici con esclusivo trattamento dei dati in forma anonima

II.5 Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

……

……

……

II.6 Durata del trattamento

La durata delle attività di trattamento, e quindi il periodo di conservazione dei dati trattati, sarà limitata alla durata dell'incarico di Servizio in essere tra le parti, in ogni caso non oltre le tempistiche previste dalla Legge. Il responsabile si impegna a cancellare (e certificare tale attività) i dati personali al termine del periodo di conservazione stabilito dal titolare.

II.7 Per il trattamento da parte di (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento

COME DA ALLEGATO IV

ALLEGATO III - Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati

NOTA ESPLICATIVA: Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

III.1 Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal responsabile 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.

(IL RESPONSABILE DEL TRATTAMENTO DEVE BARRARE LE CASELLE CORRISPONDENTI ALLE MISURE IMPLEMENTATE)

MS1 - Politiche e procedure in materia di protezione dati

□ misure idonee ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

□ procedura per il data breach, con l'istituzione di un team di risposta e gestione degli incidenti informatici (CSIRT – Computer Emergency Response, CERT – Computer Emergency Response Team) e adozione di piani di risposta agli incidenti informatici (Response Plan, Disaster Recovery Plan, Business Continuity Plan) testati e aggiornati, comprensivi di revisione delle misure di sicurezza a seguito di un attacco informatico

□ procedura per la gestione dei diritti degli interessati; controllo delle modalità con le quali vengono fornite le informazioni all'interessato (artt. 12, 13 e 14 RGPD), compreso come viene raccolto il consenso, ove necessario; comunicazione e informazioni trasparenti, efficaci (es. granulari e stratificate, comprensibili e snelle) e verificate agli interessati; pubblicizzazione di canali di comunicazione e/o punti di contatto per l'esercizio dei diritti degli interessati, richieste di chiarimento, ecc.

□ procedura per testare, verificare e valutare periodicamente l'efficacia delle misure tecniche e organizzative, con cadenza almeno annuale, al fine di procedere ad una loro rivalutazione e, se del caso, aggiornamento

□ politiche di data retention, ossia atte a monitorare la scadenza dei tempi di conservazione delle varie categorie di dati personali. La finalità del trattamento è il criterio principale per stabilire la durata del trattamento

□ Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in costante aggiornamento in relazione allo stato del progresso tecnico, certificato secondo gli Standard più diffusi

□ certificazione/garanzia di processi e prodotti (ISDP 10003, ISO 27001, ISO 31000, norme UNI, schemi di certificazione, ecc.) (indicare quali)

□ Sistema di Gestione Privacy (SGP) o altro modello organizzativo efficace e verificato (con procedure, istruzioni, registrazioni delle non conformità, ecc.)

□ nomina del Responsabile Protezione Dati (DPO)

□ controllo periodico del contenuto delle informative da fornire agli interessati

□ trasferimento di dati al di fuori dello Spazio Economico Europeo: monitoraggio se i dati sono trasferiti verso paesi terzi o organizzazioni internazionali e, in caso affermativo, se i dati godono di una protezione equivalente (con i fondamenti di legittimità su cui è basato il trasferimento, ai sensi del Capo V artt. 44 e ss. RGPD)

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS2 - Gestione del "rischio privacy" (specifico per gli Interessati)

□ Risk Assessment dei singoli trattamenti di dati personali: politiche che definiscano i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati, analisi del rischio, DPIA, ecc.

□ assessment di conformità alla normativa in materia di protezione dati personali

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS3 - Politiche di cybersecurity e analisi delle vulnerabilità

□ misure di informatica interna e di gestione e governance della sicurezza informatica (indicare ……)

□ Vulnerability Assessment

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS4 Gestione del personale (formazione, ruoli e responsabilità, gestione di eventi imprevisti)

□ nomina del personale autorizzato ai trattamenti (per iscritto)

□ adozione di Istruzioni per il trattamento/Disciplinari tecnici e policies interne che definiscano le modalità e le condizioni di utilizzo da parte del personale autorizzato dei dispositivi e dei sistemi informatici aziendali, e relativamente a:

a- uso delle postazioni, Internet, posta elettronica, utilizzo supporti removibili e documentazione cartacea

b- riutilizzo sicuro e dismissione di dispositivi elettronici e supporti

c- tutela della privacy

d- vulnerabilità informatiche (furti identità, ransomware, phishing, pretexting, keylogging, ecc.)

□ formazione dei dipendenti in merito ai metodi di riconoscimento e prevenzione degli attacchi IT e in merito agli obblighi del Reg. UE 2016/679 e delle Linee guida del Garante per la posta elettronica e internet (Del. 13/2007)

□ disattivazione di tutti gli account connessi al personale cessato e verifica della restituzione di eventuali supporti mobili, documenti etc, contenenti dati personali.

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS5 Gestione relazione con le terze parti (formalizzazione incarichi, istruzioni ai Responsabili) che accedono ai dati

□ clausole Contrattuali privacy ex art. 28, GDPR, in grado di definire con chiarezza gli obblighi dei soggetti che trattano dati personali per conto del titolare e contenenti le misure di sicurezza implementate dal Responsabile del trattamento

□ nella fase di selezione dei Fornitori, essi vengono scelti sulla base di criteri di affidabilità ed è necessario acquisire report/certificazioni sulla sicurezza

□ cifratura dei dati in base alla loro sensibilità ovvero, in assenza di cifratura, l'esistenza di procedure tali da garantire che il responsabile del trattamento non acceda ai dati affidatigli, la cifratura delle trasmissioni dei dati

(p.es.: connessioni tipo HTTPS, VPN, ecc.), garanzie in materia di protezione della rete, tracciabilità (log, audit), gestione delle autorizzazioni, autenticazione, ecc.

Qualora il responsabile sia fornitore di servizi di cloud computing:

□ definizione di: quali dati e quali trattamenti si collocheranno nel cloud; esigenze di sicurezza tecnica e giuridica; studio dei rischi al fine di individuare le misure di sicurezza adeguate; individuazione del tipo di cloud idoneo al trattamento previsto; monitoraggio gli sviluppi nel tempo.

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS6 Vigilanza (audit di conformità)

□ procedura di audit interna

□ procedura di audit esterna

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS7 Prevenzione da danni fisici e fonti di rischio non umane

□ misure di prevenzione specifiche (indicare se ci sono separazione impianti e compartimentazione antincendio, allarmi temperatura e sistemi di rilevazione e auto-spegnimento incendi, gas inerte e interruzione automatica alimentazione; sistema antincendio e idonee procedure per il loro controllo e manutenzione; allarmi anti umidità e antiallagamento sotto pavimento flottante; Impianti di condizionamento e ventilazione; filtri antipolvere e altri sistemi di pulizia; derattizzazione, ove necessario, ecc.).

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS8 Antiintrusione e controllo degli accessi fisici

□ misure di controllo degli accessi fisici (indicare se ci sono allarmi antintrusione, antifurto; porta blindata; guardiania o videosorveglianza con centrale operativa; cassaforte o armadi chiusi a chiave o stanze chiuse a chiave, procedure di accesso alle chiavi, accesso ai sistemi centrali riservato solo a personale formato e addestrato, esistenza di un referente / responsabile dell'aggiornamento dell'inventario, esistenza di un controllo degli accessi fisici da parte di dipendenti / fornitori / manutentori/ visitatori / ospiti / utenti ai locali che ospitano il trattamento (zonizzazione, accompagnamento di visitatori, assegnazione di badge, registro degli accessi, ecc.), in modo tale che i soggetti che accedono ai documenti sono identificati e identificabili, ecc.)

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS9 Lotta contro il malware

□ misure antimalware (indicare ……)

□ il SO, il suo firewall e l'antivirus sono periodicamente aggiornati e configurati con le opportune estensioni che consentano la rilevazione di malware e la navigazione sicura

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS10 Sicurezza dei siti web e APP

Soltanto qualora il responsabile crei, implementi o gestisca per il titolare PIATTAFORME DIGITALI, SITI WEB o APP:

□ utilizzo di soluzioni provenienti da fornitori affidabili;

□ controlli periodici della sicurezza (site-check);

□ crittografia del sito con un certificato "Secure Socket Layer" (SSL) e utilizzare il linguaggio di markup HTTPS, che permettono trasferimenti di dati in sicurezza;

□ possibilità, per gli utenti, di attivare l'autenticazione a due fattori (anche per le caselle di posta elettronica), laddove ciò sia possibile;

□ protezione dell'accesso al sito con credenziali mediante un sistema di blocco IP (ad es. se viene inserito per 5 volte un nickname non esistente o per 10 volte una password non corretta), imponendo agli utenti l'utilizzo di password sicure ed univoche;

□ utilizzo delle ultime versioni dei browser e dei software (CMS, Wordpress, PHP, ecc.);

□ integrazione dei "captcha", laddove ciò sia possibile;

□ pubblicazione dei dati aziendali sul sito web, per come richiesto dalla normativa in materia;

□ backup completo, dei file e del Database, effettuato in maniera regolare;

□ presenza di firewall che blocca eventuali iniezioni di codice esecutivo;

□ blocco di tutte le funzioni che permettono l'ottenimento di informazioni di versioni e utenti.

□ con riferimento alle autorizzazioni richieste all'utente da un'APP, le autorizzazioni sono soltanto quelle indispensabili per l'utilizzo dell'APP, come richiesto dal principio di minimizzazione dei dati personali enunciato nell'art. 5, par. 1, lett. c) del Reg. UE 2016/679, poiché spesso, ad esempio, non sono indispensabili l'accesso a: posizione dell'utente, fotocamera, contatti, microfono, spazio di archiviazione (file presenti nello smartphone).

□ con riferimento, invece, ai cookie dei siti web o delle APP, conformemente alle Linee Guida del Garante del 10 giugno 2021[7] sono previsti accorgimenti necessari a:

□ anonimizzare i dati personali, ove necessario (es. verificare che i file di registro nei server web non contengano dati personali come, ad esempio, l'indirizzo IP)

□ evitare l'utilizzo di identificatori utente univoci;

□ procedere a trasferimenti dei dati personali al di fuori dell'UE soltanto previa autorizzazione del titolare e dopo adeguato Transfer Impact Assessment (TIA) teso a verificare il rispetto del Capo V del GDPR;

□ informare gli utenti ai sensi dell'art. 13, Reg. UE 2016/679, prima di trattare i dati (indicando le basi giuridiche del trattamento);

Laddove sia necessario il consenso dell'utente come base giuridica del trattamento (ad es. per l'installazione di cookie analitici o di profilazione, per trattamenti di dati a fini di marketing, ecc.):

□ sistema di raccolta (e conservazione) del consenso esplicito dell'utente, in maniera corretta e trasparente;

□ banner per la raccolta del consenso, conforme alle Linee Guida del Garante del 10 giugno 2021, che dia la possibilità, ai visitatori, di modificare o revocare il consenso;

□ assenza di cookie wall, processi di scrolling e consensi flaggati di default.

Laddove siano presenti form che possono essere compilati dagli utenti del sito web:

□ flag obbligatorio, per l'utente, su "Ho preso visione dell'informativa privacy" prima di poter inviare i dati.

[7] GARANTE PRIVACY, Provvedimento 10 giugno 2021, n. 231, "Linee guida cookie e altri strumenti di tracciamento" (doc. web n. 9677876, pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021), che aggiorna il precedente Provvedimento dell'8 maggio 2014, n. 229, avente ad oggetto "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie"

N.B. Poiché il titolare elabora una propria policy per il sito web o per l'APP, è necessario che il responsabile del trattamento comunichi allo stesso titolare: le modalità del trattamento, le misure di sicurezza tecniche del sito o dell'APP, se vi è un trasferimento di dati al di fuori dell'UE, nonché una tabella con l'elenco dei cookie installati dal sito o dall'APP sul pc dell'utente, indicando, in particolare, il nome, la finalità, la durata, lo scopo, e se si tratta di cookie anonimo o univoco.

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS11 Sicurezza di server, database, reti, Wi-Fi

In osservanza del Reg. UE 2016/679, del novellato D. Lgs. n. 196/2003 e delle Linee guida del Garante del 24 luglio 2008, il responsabile del trattamento adotta idonei accorgimenti tecnici volti ad incrementare il livello di sicurezza dei dati, con particolare riferimento alle operazioni di registrazione e gestione con strumenti elettronici dei dati personali.

□ protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la trasmissione elettronica dei dati

□ gestione dei server, degli apparati di rete e del Wi-Fi

□ ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione è crittografata tramite idonei protocolli (TLS / SSL)

□ idonei sistemi di autenticazione e di autorizzazione per i soggetti autorizzati al trattamento, in funzione dei ruoli e delle esigenze di accesso e trattamento

□ procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti autorizzati al trattamento

□ sistemi di audit log per il controllo degli accessi ai database e per il rilevamento di eventuali anomalie, con inoltro a un server di log centrale

□ server ove risiedono database e applicazioni configurati per essere operativi utilizzando un account separato, con i privilegi minimi

□ idonee misure di crittografia dei dati (at rest) e dei dati in transito

□ aggiornamento di firmware, sistemi operativi e software presenti sui server, dispositivi client, componenti attivi della rete, nonché tutti gli ulteriori dispositivi che operano sulla stessa linea di rete

□ progettazione e organizzazione dei sistemi informatici in modo tale da segmentare e isolare i sistemi e le reti contenenti i dati, al fine di evitare che il malware si propaghi all'interno delle strutture o verso sistemi esterni all'organizzazione

□ installazione di software anti-malware, firewall e sistema di detenzione e prevenzione delle intrusioni

□ penetration test periodici

□ firewall, sonde anti-intrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete (es. MAC Address Binding per rete cablata wireless, Wifi con protezione crittografica e registrazione e logging utenti, Firewall di rete e Appliance con content filtering, Gestione Pathing e Updates su routers, firewalls, switches, ecc.)

□ la policy dell'Organizzazione vieta hotspot con smartphone personali

□ i sistemi di cablaggio rete e gli Impianti di comunicazione wireless sono certificati

□ connessioni WIFI separate per uso interno e per gli ospiti

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS12 Sicurezza di hardware, postazioni e dispositivi

□ firewall e antivirus installati su ogni dispositivo

□ misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita

□ laddove siano utilizzati sistemi di memorizzazione o archiviazione dei dati, sono implementati idonei accorgimenti per garantire la protezione dei dati registrati dai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati)

□ esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.)

□ gli utenti non hanno i privilegi per installare o disattivare applicazioni software senza autorizzazione

□ attivazione del timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo

□ sistema di hardware monitoring (con allarmi per surriscaldamenti, guasti componenti, ecc.)

□ sistemi/supporti portabili in caso di evacuazione

□ utilizzo di lucchetti / protezioni antitheft su postazioni mobili e valigette, zaini, ecc.

□ auditing sulle postazioni utente, sui sistemi operativi, sulle applicazioni

□ esistenza e aggiornamento costante di un registro delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hw, sw e rete)

□ procedure di smaltimento di hardware e altri supporti di memoria contenenti dati personali, idonee a rendere impossibile il recupero di dati

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS13 Sicurezza dei software

□ procedure di aggiornamento periodico e automatico dei software di sicurezza

□ inventario dei software autorizzati

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS14 Manutenzione

□ prevenzione di malfunzionamenti e problemi tecnici dei sistemi

□ politica di manutenzione fisica dei dispositivi, compresa la manutenzione remota, ove autorizzata, con specifica attenzione ai metodi di gestione dei materiali difettosi

□ manutenzione interna periodica di sistemi e di reti (backup configurazioni, verifica firmware, prestazioni hardware, capienza dischi, utilizzo risorse, ecc.)

□ contratti di di manutenzione e assistenza hardware e software attivi

□ possibilità di effettuare manutenzioni pianificate senza impatti negativi sulla gestione della funzionalità

□ installazione regolare di aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

MS15 Backup e Restore

□ misure idonee a ripristinare immediatamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico e politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.)

□ procedura di backup aggiornata, sicura e testata, con separazione tra i dispositivi utilizzati per i backup a lungo termine e quelli a medio termine, oltre che rispetto a terze parti

□ procedure di backup e ripristino dei dati definite, documentate e chiaramente collegate a ruoli e responsabilità

□ backup completi eseguiti regolarmente

□ monitoraggio dell'esecuzione dei backup per garantirne la completezza

□ copie del backup conservate in modo sicuro in luoghi diversi

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

MS16 Business continuity

□ business continuity con utilizzo di gruppi di continuità, UPS, stabilizzatori, al fine di garantire la continuità delle attività e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità. Indicare, in particolare, se vengono implementati:

□ identificazione, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità

□ piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative

□ preparazione e divulgazione di procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità

□ test periodici per tutti i componenti del piano di continuità

□ mantenimento e aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

MS17 Disaster recovery

□ disaster recovery ("recupero dal disastro"): definizione dei requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in seguito a eventi disastrosi

□ Disaster Recovery Plan (DRP) contenente l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività.

Note ulteriori:

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS18 Controllo degli accessi logici, autenticazione, password

□ accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi;

□ sistemi che costituiscono l'infrastruttura ICT opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

□ Adozione di una procedura di autenticazione per accedere ai dispositivi informatici, attraverso "credenziali personalizzare di autenticazione", che consistono in un user - ID associato a una parola chiave segreta (password di almeno 8 caratteri contenente obbligatoriamente almeno una lettera maiuscola, un numero e un carattere speciale; previsione, ove necessario, di un meccanismo di rinnovo periodico della password).

□ Adozione di forme forti di criptazione o di autenticazione per gli accessi amministrativi ai sistemi IT, come l'autenticazione a due fattori, oltre a un sistema di gestione delle password.

□ Custodia delle credenziali di autenticazione, che devono essere utilizzate in modo pertinente e strettamente personale e non essere comunicate ad altri soggetti, neppure se parimenti autorizzati al trattamento, al fine di minimizzare i rischi di accesso illeciti e utilizzi impropri delle stesse.

Soltanto qualora il responsabile crei, implementi o gestisca per il titolare **CASELLE DI POSTA ELETTRONICA:**

□ comunicazione al titolare ogni singola attivazione di una nuova casella di posta elettronica;

□ sistema di password forte.

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS19 Gestione dei profili di accesso

□ processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso

□ autorizzazioni di accesso alle informazioni differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e periodicamente sottoposte a revisione

□ accesso alle informazioni da parte di ogni singolo utente limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (c.d. principio del "need to-know")

□ comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, fondata sullo stesso principio

□ rimozione delle autorizzazioni di accesso non appena un utente cessi di essere abilitato ad accedere a una risorsa locale o IT, ovvero allo scadere del contratto

□ revisione annuale delle abilitazioni per identificare ed eliminare gli account non utilizzati e riallineare i privilegi concessi alle funzioni di ciascun utente

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS20 Tracciabilità (Logging) degli eventi

□ logging delle operazioni sui dati (creazione, lettura, estrazione, modifica, cancellazione) che consente di registrare le operazioni effettuate sul sistema informatico, al fine di identificare un accesso abusivo ovvero un utilizzo abusivo di dati personali, oppure per stabilire la causa di un incidente

□ attività degli Amministratori di Sistema registrate tramite log conservati nel rispetto del Provv. Garante 2008

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS21 Minimizzazione dei dati

□ filtraggio e rimozione dei metadati

□ riduzione del potenziale identificativo o del carattere "particolare" del dato

□ riduzione dell'accumulazione dei dati

□ limitazione dell'accesso ai dati oppure controllo degli accessi ai dati "particolari" o crittografia dei dati "particolari"

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS22 Altre misure applicate ai dati

□ pseudonimizzazione e mascheramento dei dati, laddove applicabile, qualora non sia necessaria l'identificazione diretta del soggetto i cui dati si riferiscono, in modo che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente

□ crittografia di files e database, anche su dispositivi portatili e supporti removibili

(descrivere i mezzi implementati per assicurare la confidenzialità dei dati archiviati, così come le procedure per gestire chiavi crittografiche quali creazione, archiviazione, aggiornamento in caso di sospetta compromissione ecc.)

□ anonimizzazione (indicare i meccanismi implementati, le garanzie introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati)

□ partizionamento dei dati (indicare i metodi utilizzati)

□ misure di protezione dei dati durante la trasmissione

□ misure per garantire la qualità dei dati

□ misure per consentire la portabilità dei dati e garantire la cancellazione

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS23 Archiviazione sicura (nella consegna, sistemazione, consultazione) e dismissione sicura

□ politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.)

□ procedure per la dismissione sicura delle apparecchiature informatiche a fine vita, al fine di evitare il recupero di informazioni da supporti o media dismessi (principalmente memorie di massa)

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

MS24 Archiviazione sicura dei documenti cartacei (stampati, archiviati, distrutti e scambiati) e dismissione sicura

Soltanto qualora il responsabile svolga per il titolare TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI:

□ conservazione di atti e documenti su supporto cartaceo contenenti dati personali in archivi o locali ad accesso autorizzato e riservato e custodia con diligenza, in maniera tale che le persone non autorizzate al trattamento non possano venirne a conoscenza, neppure accidentalmente (es. non lasciare documenti incustoditi sulla scrivania)

□ duplicazione di atti e documenti contenenti dati personali da evitare, laddove non strettamente necessaria; in caso di duplicazione, conservazione della copia cartacea o del supporto fisico su cui è memorizzata la copia in forma elettronica con le medesime modalità degli originali cartacei, al fine di assicurarne la riservatezza e integrità

□ qualora necessario, distruzione di atti e documenti contenenti dati personali e utilizzo di appositi strumenti o modalità che ne impediscano il ricomponimento e il successivo utilizzo

Note ulteriori:

(Descriva la Società ulteriori specifiche riferite alle misure sopra richiamate)

_____

_____

III.2 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.

NESSUNA

III.3 Amministratori di Sistema

Con riferimento alle vigenti prescrizioni con riguardo all'attribuzione delle funzioni di "Amministratore di Sistema" (Provvedimento del Garante "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27/11/2008 e ss. mm. ii.), il Responsabile indichi nome, cognome, indirizzo di posta elettronica, contatto telefonico di ogni singolo Amministratore di Sistema:

_____

_____

ALLEGATO IV - Elenco dei sub-responsabili del trattamento

NOTA ESPLICATIVA: Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a), opzione 1], e *comprendere una chiara delimitazione delle responsabilità qualora siano autorizzati più sub-responsabili del trattamento.*
Si ricorda che, ai sensi dell'art. 28, par. 4, GDPR, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

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

Nome: ……
Indirizzo: ……
Nome, qualifica e dati di contatto del referente: ……
Descrizione del trattamento (parte del trattamento interessata, ciclo di vita dei dati, categorire di dati trattati, categorire di interessati, tempi di conservazione dei dati, ecc.):
……
……
……
misure tecniche e organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento:
……
……
……
……

Nome: ……
Indirizzo: ……
Nome, qualifica e dati di contatto del referente: ……
Descrizione del trattamento (parte del trattamento interessata, ciclo di vita dei dati, categorire di dati trattati, categorire di interessati, tempi di conservazione dei dati, ecc.):

.....
.....
.....
misure tecniche e organizzative specifiche che il (sub-)responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento:
.....
.....
.....
.....

ALLEGATO V - Modulo da utilizzare da parte del responsabile in caso di necessità di segnalazione al titolare di un sospetto data breach

Data	
Nome e cognome del segnalante	
Struttura di afferenza, funzione e dati di contatto del segnalante (tel., e-mail ecc.)	
Ulteriori soggetti coinvolti nel trattamento	
Informazioni sul data breach	
1. Momento in cui è avvenuta la violazione	☐ Il _____ ☐ Dal _____ (la violazione è ancora in corso) ☐ Dal _____ al _____ ☐ In un tempo non ancora determinato
2. Modalità con la quale il responsabile del trattamento è venuto a conoscenza della violazione	
3. Momento nel quale il responsabile del trattamento è venuto a conoscenza della violazione (e motivi del ritardo, se la segnalazione è inviata dopo il termine di 24 ore)	
4. Tipo di violazione	☐ Ransomware
	☐ Lettura (presumibilmente i dati non sono stati copiati)
	☐ Copia (i dati sono ancora presenti sui sistemi)
	☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
	☐ Cancellazione (i dati non sono più sui sistemi e non li ha neppure l'autore della violazione)
	☐ Furto (i dati non sono più sui sistemi e li ha l'autore della violazione)
	☐ Altro:_____(*DESCRIVERE*)

5. Natura della violazione dal punto di vista del RID	☐ Perdita di riservatezza del dato personale (R) ☐ Perdita di integrità del dato personale (I) ☐ Perdita di disponibilità del dato personale (D)
6. Causa della violazione	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta
7. Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione	
8. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti	
9. Categorie di interessati coinvolti nella violazione	☐ Dipendenti/Consulenti ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) ☐ Associati, soci, aderenti, simpatizzanti, sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐ Altro _____
10. Numero (anche approssimativo) di interessati coinvolti nella violazione.	☐ N. ___ interessati ☐ Circa n. ____ interessati ☐ Non determinabile ☐ Non ancora determinato
11. Categorie di dati personali oggetto di violazione	☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…) ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza ☐ Dati di profilazione ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) ☐ Dati di localizzazione ☐ Dati che rivelino l'origine razziale o etnici ☐ Dati relativi a opinioni politiche ☐ Dati relativi a convinzioni religiose o filosofiche ☐ Dati che rivelino l'appartenenza sindacale ☐ Dati relativi alla vita sessuale o all'orientamento sessuale ☐ Dati relativi alla salute ☐ Dati genetici ☐ Dati biometrici ☐ Altro _____ ☐ Categorie ancora non determinate

12. Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione	☐ N.0 ☐ Circa N. ☐ Non determinabile ☐ Non ancora determinato
13. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati	
Probabili conseguenze della violazione	
1. Probabili conseguenze della violazione per gli interessati	**In caso di perdita di riservatezza:** ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di integrità:** ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro _____ ☐ In corso di valutazione **In caso di perdita di disponibilità:** ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro _____ ☐ In corso di valutazione Eventuali ulteriori considerazioni sulle conseguenze della violazione: _____
2. Potenziale impatto per gli interessati	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti ☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo _____ ☐ Non ancora definito
3. Gravità del potenziale impatto per gli interessati	☐ Trascurabile ☐ Bassa ☐ Media ☐ Alta ☐ Non ancora definita _____
Misure adottate a seguito della violazione (o di cui si propone l'adozione)	
1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati	

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future	