**DATA PROTECTION AGREEMENT**

**ai sensi dell’art. 28 del Regolamento Europeo (GDPR) n. 679/2016**

***(Regolamento 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)***

**TRA**

L’Azienda Ospedaliero Universitaria “SS. Antonio e Biagio e C. Arrigo” di Alessandria, in persona del suo Direttore Generale (di seguito Azienda o Titolare), con sede legale in Via Venezia, 16 – 15121 Alessandria, in qualità di Titolare del trattamento ai sensi dell’art.24 del Regolamento Europeo 2016/679 (di seguito GDPR)

E

**Il fornitore…………………………………… con sede in ……………………………………………………………………. P.Iva………………………………………. C.F. …………………………………………………, in persona di ………………………….………………………………………..**

.

Premesso che:

* 1. Xxxxxxxxxxxxxxxxxxxxxxxxx (di seguito Responsabile), ha in essere con l’Azienda un contratto di ……………………………………………………………………………………………………………………………….. (precisare oggetto e delibere di affidamento) con decorrenza dal ……………………………………………. al ………………………………………….;
  2. le attività oggetto del contratto comportano il trattamento di dati personali come definiti dall’art.4 n. 1) del GDPR dei quali è Titolare l’Azienda, e meglio elencati nell’Appendice 1;
  3. l’art. 28 del GDPR attribuisce al Titolare del trattamento la facoltà di ricorrere ad un Responsabile che presenti, per esperienza, capacità ed affidabilità, garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza e garantisca la tutela dei diritti dell’interessato;
  4. il Responsabile dichiara di possedere e fornisce delle evidenze a dimostrazione della competenza qualificata per garantire il rispetto delle disposizioni vigenti in materia di privacy, e l'attuazione degli obblighi derivanti dal presente contratto (SE POSSIBILE DOCUMENTARE ad es. adesione a codici deontologici ovvero a schemi di certificazione, ovvero esibizione di procedure interne di gestione dei dati quali DPIA o documento di verifica della compliance al GDPR o indicazione della pagina internet dove si possono reperire i documenti inerenti la privacy);
  5. il Responsabile dichiara altresì di aver adottato e di impegnarsi a mantenere per tutta la durata del servizio le misure tecniche e organizzative dettagliate nell’Appendice al presente atto, per garantire un livello di sicurezza adeguato rispetto ai rischi che corrono i dati e che derivano da distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o trattati;
  6. ai sensi dell’art. 28.3 del GDPR i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;
  7. con il presente Data Protection Agreement (DPA), il fornitore assume il ruolo di Responsabile del trattamento e si impegna ad effettuare, per conto del Committente, le operazioni di trattamento di seguito definite, nel rispetto del GDPR e del Codice Privacy;
  8. le Parti si impegnano a garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del GDPR, tenendo anche conto di quanto contenuto nelle “*clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento*” emanate con Decisione di Esecuzione (UE) 2021/915 della Commissione Europea del 4 giugno 2021.

Tutto ciò premesso,

il Responsabile per quanto concerne il trattamento dei dati derivante dall’esecuzione del servizio in oggetto, dovrà attenersi alle disposizioni contenute nel GDPR 2016/679, nel D.Lgs. n.196/2003 e ss.mm.ii., e operare nel rispetto dei principi espressi dalle norme in materia di trattamento di dati personali, sensibili (o particolari) e giudiziari, ai provvedimenti emanati dal Garante e a tutte le prescrizioni qui di seguito fornite dal Titolare e a quelle successive che il Titolare del trattamento, riterrà di dettare, senza oneri aggiuntivi per quest’ultimo.

Il Responsabile del trattamento dati, nei limiti della materia disciplinata, della durata del trattamento, della natura e della finalità del trattamento, del tipo di dati trattati e delle categorie di interessati esplicitati nel contratto/convenzione di cui in premessa nonché nel presente atto, deve:

1. svolgere le attività di trattamento solamente su istruzione documentata del Titolare e informare immediatamente il Titolare nel caso in cui tali istruzioni violino, a suo parere, il GDPR o le disposizioni applicabili relative alla protezione dei dati;
2. trattare i dati personali per le sole finalità specificate e nei limiti dell’esecuzione delle prestazioni contrattuali e per la sola durata del contratto stesso;
3. adottare le misure tecniche ed organizzative di sicurezza dei dati personali e particolari adeguate alla/e tipologia/e di trattamento e condivise formalmente con il Titolare, idonee a salvaguardare la riservatezza, disponibilità e integrità dei dati trattati, ai sensi di quanto disposto dall’art 32 del GDPR. In particolare – in considerazione dello stato dell’arte, dei costi di attuazione, della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche, del rischio derivante da distruzione, perdita, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative previste dal D.Lgs. n. 82/2005 e ss.mm.ii, dalle norme AGID (linee guida AGID circa le “Misure minime di sicurezza ICT per le pubbliche amministrazioni”) e dalle disposizioni normative e regolamentari in materia, nonché ad ottemperare a tutti i provvedimenti dell’European Data Protection Board (EDPB) e del Garante Privacy applicabili, in particolare quello relativo agli amministratori di sistema. In particolare, si impegna ad implementare le misure elencate nell’appendice e a rivalutarle periodicamente e ogni qualvolta si ravvede una variazione dell’efficacia delle stesse o del livello di rischio iniziale;
4. adottare politiche interne e attuare, per quanto di sua competenza, in relazione alla tipologia di prestazione/trattamento da eseguire, misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);
5. individuare e nominare per iscritto le persone fisiche autorizzate al trattamento dei dati, ai sensi dell’art. 29 del GDPR e dell’art. 2 quaterdecies del D.Lgs. 196/2003, fornendo loro le istruzioni operative specifiche alle quali devono attenersi nell’espletamento dell’attività di trattamento;
6. concedere l’accesso ai dati personali unicamente ai soggetti autorizzati al trattamento ai sensi dell’art. 29 del GDPR nella misura strettamente necessaria per l'attuazione e la gestione delle attività oggetto dei trattamenti e a garantire che gli stessi abbiano ricevuto la formazione necessaria e le istruzioni dettagliate finalizzate a trattare in modo sicuro e riservato i dati affidati, custodendoli e controllandoli nel modo più appropriato
7. garantire la riservatezza dei trattamenti, anche vincolando alla riservatezza non solo per la durata del contratto, ma anche per tutto il tempo successivo, senza limiti temporali, le persone fisiche autorizzate al trattamento e impegnando loro e chiunque agisca sotto la sua responsabilità e abbia accesso ai dati personali a non trattare tali dati se non per le finalità del trattamento e comunque dopo averli istruiti adeguatamente;
8. non ricorrere ad un altro responsabile (sub responsabile) senza previa autorizzazione scritta, specifica o generale del titolare del trattamento secondo quanto previsto dall’art. 28.2 del GDPR. Alla data della sottoscrizione del presente atto, il Titolare autorizza il ricorso ai sub-Responsabili riportati in Appendice.

Il sub-Responsabile del trattamento deve rispettare gli stessi obblighi ai quali è assoggettato il Responsabile. Spetta al Responsabile assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l’adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del GDPR.

In caso di violazione da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti. Il Titolare potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit, verifiche e ispezioni, anche avvalendosi di soggetti terzi.

Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l’applicazione del Regolamento, o risulti che il sub-Responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare, quest’ultimo diffiderà il Responsabile a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine non superiore a 7 giorni lavorativi. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell’art. 1454 c.c., l’Azienda potrà, in ragione della gravità della condotta del sub-Responsabile e fatta salva la possibilità di fissare un ulteriore termine per l’adempimento, risolvere il contratto con il Responsabile, salvo il risarcimento del danno.

In alternativa alle verifiche di cui sopra, il Titolare potrà richiedere al Responsabile di fornire annualmente, o comunque su sua richiesta, una relazione sull’andamento della gestione dei dati personali e sull’applicazione delle misure di sicurezza approvate da parte del sub-Responsabile autorizzato;

1. non trasferire tutti (o alcuni) dati personali derivanti dall’attività oggetto del contratto verso un paese terzo o un’organizzazione internazionale, senza autorizzazione del Titolare, l’indicazione della base legale che legittima il trasferimento e l’indicazione di idonei meccanismi di trasferimento; l’eventuale trasferimento di dati personali verso un paese terzo (extra UE) o un’organizzazione internazionale è in ogni caso ammesso solo se conforme agli artt. 44 e ss. del GDPR specificando che dovranno essere garantite da parte del responsabile misure tecniche e organizzative adeguate al fine di proteggere i diritti dei terzi interessati, l’esistenza di meccanismi di trasferimento tracciati e la documentazione delle opportune misure di sicurezza messe in atto;
2. notificare al titolare del trattamento tramite pec all’indirizzo [asoalessandria@pec.ospedale.al.it](mailto:asoalessandria@pec.ospedale.al.it) immediatamente e comunque entro il primo giorno lavorativo successivo, qualunque richiesta ricevuta inerente l’esercizio dei diritti degli interessati ai sensi degli artt. 15 e ss. del GDPR, evitando di rispondere alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare, al quale dovrà comunque prestare assistenza per consentirgli di evadere le richieste;
3. impegnarsi, su richiesta del Titolare, al termine della prestazione dei servizi oggetto del contratto, a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l’adempimento di tale operazione e, qualora richiesto, alla restituzione dei dati al Titolare unitamente a qualsiasi documento o mezzo contenente detti dati, ai sensi dell’art. 28 paragrafo g) del GDPR;
4. mettere a disposizione del Titolare del trattamento, nel rispetto del principio di rendicontazione (accountability), tutta la documentazione e/o certificazione riguardante le misure di sicurezza adottate necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, ispezioni e audit - previo congruo preavviso se eseguiti presso la sede del Responsabile - circa l’adeguatezza e l’efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

Nel caso in cui all’esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l’applicazione del Regolamento, o risulti che il Responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare, quest’ultimo diffiderà il Responsabile ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all’occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell’art. 1454 c.c., l’Azienda potrà, in ragione della gravità della condotta del Responsabile e fatta salva la possibilità di fissare un ulteriore termine per l’adempimento, risolvere il contratto, salvo il risarcimento del danno. In alternativa alle verifiche di cui sopra, il Titolare potrà richiedere al Responsabile di fornire annualmente, o comunque su sua richiesta, una relazione sull’andamento della gestione dei dati personali e sull’applicazione delle misure di sicurezza approvate;

1. prestare tutta la necessaria collaborazione e disponibilità, per quanto di competenza, a fronte di richieste di informazioni, controlli ed accessi da parte del Garante, di altre pubbliche autorità competenti, avvisando contestualmente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell’Autorità Garante per la protezione dei dati personali; inoltre, deve assistere, inoltre, per quanto di sua competenza, il Titolare nel caso di richieste formulate dall’Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del contratto in essere;
2. tenere ed aggiornare periodicamente un Registro delle attività di trattamento effettuate sotto la propria responsabilità ai sensi dell’art. 30 del GDPR e cooperare con il Titolare e con l’Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione dell’Autorità e del Titolare, laddove ne venga fatta richiesta ai sensi dell’art. 30.4 del GDPR.
3. informare tempestivamente e, in ogni caso, senza ingiustificato ritardo dall’avvenuta conoscenza, il Titolare di ogni incidente di sicurezza, violazione o sospetta violazione di dati personali (c.d. data breach) tramite una formale comunicazione scritta a ciascuno dei seguenti indirizzi:

* [asoalessandria@pec.ospedale.al.it](mailto:asoalessandria@pec.ospedale.al.it) (Titolare)
* [dpo@ospedale.al.it](mailto:dpo@ospedale.al.it) (DPO dell’Azienda)

Tale notifica da effettuarsi tramite il modulo riportato in Appendice al presente atto, è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all’Autorità Garante per la protezione dei dati personali entro i termini previsti dal GDPR; nel caso in cui il Titolare debba fornire informazioni aggiuntive all’Autorità di controllo, il Responsabile del trattamento si impegna a supportare il Titolare nell’ambito di tale attività.

Il Responsabile deve mantenere un registro degli incidenti di sicurezza, anche qualora non vi siano violazioni, così come previsto dall’art. 33.5 del GDPR.

In ogni caso il Responsabile dovrà informare il DEC dell’Azienda per coordinare le azioni di mitigazione del rischio, contenimento dei danni, individuazione delle misure di sicurezza da adottare.

A seguito del verificarsi di detti incidenti il Titolare potrà fare attività di audit, anche senza preavviso e avvalendosi di soggetti terzi.

Nel caso in cui alla conclusione di tali verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate, Azienda Ospedaliera “SS. Antonio e Biagio e C. Arrigo” di Alessandria, potrà:

* prescrivere ulteriori misure di sicurezza, anche apportando modifiche a quelle in essere, con particolare riferimento al presente accordo;
* far rispondere il Responsabile del trattamento del danno causato, fino alla risoluzione del contratto, a meno che il Responsabile stesso non dimostri che l’evento dannoso non gli sia in alcun modo imputabile;

1. su eventuale richiesta del Titolare, assistere quest’ultimo, per quanto di competenza, nello svolgimento della valutazione d’impatto sulla protezione dei dati, conformemente all’art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall’art. 36 del medesimo GDPR;
2. comunicare tempestivamente al Titolare del trattamento dati eventuali variazioni che richiedano un adeguamento del presente atto;
3. informare tempestivamente e adeguatamente il Responsabile della Protezione dati (RPD o DPO) dell’Azienda per tutte le questioni riguardanti la protezione dei dati;

Ai sensi dell’art. 37 GDPR le parti indicano qui di seguito i recapiti dei rispettivi DPO (o RPD):

per l’Azienda: Dr.ssa Silvia Straneo tel. 0131/206710 email: [dpo@ospedale.al.it](mailto:dpo@ospedale.al.it)

per il Responsabile:

………………………………………………………………………………………………………………………………………

Per tutte le controversie che dovessero sorgere con riferimento al presente Accordo sarà esclusivamente competente il Foro di Alessandria.

Il trattamento dei dati (finalità del trattamento, tipo di dati personali trattati, operazioni eseguite sui dati, categorie di interessati), in esecuzione del contratto principale suindicato, è specificato nell’appendice.

Letto, approvato e sottoscritto digitalmente

1. per l’Azienda Ospedaliero Universitaria “SS. Antonio e Biagio e C. Arrigo” di Alessandria

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. per il Responsabile

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ai sensi e per gli effetti dell’art. 1341 c.c. il Responsabile dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli oggetto della presente Nomina e negli allegati

Letto, approvato e sottoscritto digitalmente

1. per il Responsabile

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendice 1**

**SPECIFICHE DEI TRATTAMENTI DELEGATI AL RESPONSABILE**

I trattamenti delegati al Responsabile da parte del Titolare sono i seguenti (in caso di più trattamenti occorre compilare una tabella per ciascun trattamento):

|  |  |  |
| --- | --- | --- |
| **Titolare del trattamento** |  |  |
| **Descrizione del Trattamento** |  | SPECIFICARE |
| **Durata massima** |  | * Sino al termine del periodo contrattuale ed eventuali ulteriori rinnovi come da specifiche di contratto. * Specificare se diversa dalla durata del contratto |
| **Finalità** |  | SPECIFICARE |
| **Tipo di dati personali trattati** |  | * Dati personali e personali identificativi: (es: nome, cognome, CF, data e luogo di nascita, ecc….) * Dati personali particolari relativi allo stato di salute * SPECIFICARE EVENTUALI ALTRI |
| **Categorie di interessati** |  | * Pazienti * Pazienti minori di età * Dipendenti dell’Azienda * Personale esterno * SPECIFICARE EVENTUALI ALTRI |
| **Operazioni di trattamento** |  | * Raccolta, registrazione, consultazione * SPECIFICARE EVENTUALI ALTRI |
| **Tempo di conservazione dei dati personali trattati** |  | * Esplicitare se diverso dalla durata del contratto |
| **Misure di sicurezza specifiche da adottare** |  | Il Responsabile per il trattamento impiega:   * Istruzioni sulla gestione delle credenziali di autorizzazione e accesso * Istruzione e formazione del personale * Nonché tutte le MISURE TECNICHE, procedurali e logistiche sulla sicurezza del trattamento dettagliate in appendice 2) |
| **Elenco dei Subresponsabili art. 28 par.4** |  | * Non impiegati * Specificare, se impiegati, ragione sociale, ambito di attività e dati di contatto |

**Allegato 2**

**MISURE DI SICUREZZA**

Il Responsabile adotta le misure tecniche ed organizzative di sicurezza dei dati personali e particolari, adeguate e specifiche alla/e tipologia/e di trattamento/i come indicate in … (es nell’offerta tecnica presentata e/o nella documentazione prodotta) o indicate tra quelle nella tabella allegata.

Misure organizzative, tecniche, procedurali e logistiche sulla sicurezza nei trattamenti: per garantire la disponibilità, la riservatezza, l’integrità e la tutela dei dati degli interessati, ai fini di mitigare i seguenti rischi:

* + - distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
    - trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
    - interruzione della disponibilità dei dati involontaria o volontaria (dolosa);

sono implementate le misure di seguito elencate, scelte 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. Tutte le misure di sicurezza sono rivalutate periodicamente e ogni qualvolta si ravvede una variazione dell’efficacia delle stesse o del livello di rischio iniziale.

Nelle tabelle seguenti mantenere solo le righe corrispondenti alle misure adottate ed eliminare le righe corrispondenti a quelle non adottate

Misure di sicurezza organizzative adottate dal Responsabile:

|  |  |
| --- | --- |
| **Misura** | **Descrizione/Esempi** |
| **Formazione e sensibilizzazione del personale** | Sono eseguiti gli interventi formativi previsti nel piano di formazione in materia di protezione dei dati definito annualmente |
| **Istruzioni per il trattamento** | Sono fornite agli autorizzati le istruzioni dettagliate sul trattamento dei dati (regole da applicare, manuali di organizzazione del servizio, disciplinare per l’uso degli strumenti aziendali, ecc.) |
| **Definizione di regole di archiviazione** | Sono definiti la politica e i processi di gestione dell'archivio cartaceo che contiene dati personali (consegna dei documenti, archiviazione, consultazione, ecc.) |
| **Definizione del modello organizzativo** | Sono definite regole e responsabilità a livello aziendale in materia di sicurezza e privacy e a livello di ruoli e responsabilità del progetto o servizio (es. modello organizzativo di gestione della privacy, regolamento privacy, codice etico, manuale dei profili professionali)  Sono definite processi, procedure e linee guida per la protezione dei dati personali (es. gestione del registro, gestione delle violazioni dei dati personali, gestione dei diritti degli interessati, gestione degli audit) |
| **Audit** | Sono eseguiti gli audit previsti nel piano di audit definito annualmente |
| **Regolamentazione delle misure applicate nei rapporti con i fornitori** | I contratti con i fornitori che trattano i dati includono istruzioni dettagliate in materia di protezione dei dati |
| **Predisposizione di un modello per l'analisi dei rischi di privacy/sicurezza e PBDD** | È adottato un modello per l'analisi, la valutazione e il trattamento dei rischi di sicurezza e privacy e un modello per documentare l’applicazione dei principi di privacy by design e by default (PBDD) |
| **Documentazione del software e del servizio** | Sono predisposti e aggiornati i documenti di progettazione, architettura, installazione del software utilizzato (es. vista d'insieme, documento di architettura, deploy, ecc.) e per la gestione del servizio |

Misure di sicurezza tecniche trasversali adottate dal Responsabile:

| **Misura** | **Descrizione/Esempi** |
| --- | --- |
| **Armadi e contenitori dotati di serrature** | Sono disponibili contenitori per la conservazione sicura, dotati di serratura |
| **Armadi, casseforti e contenitori ignifughi** | Sono disponibili contenitori ignifughi per la conservazione sicura |
| **Misure antincendio** | L'edificio in cui si svolge il trattamento è dotato di misure antincendio di protezione dei beni e dei documenti |
| **Sistemi di sorveglianza** | L'edificio in cui si svolge il trattamento è dotato di misure di controllo accessi ai locali e di videosorveglianza |
| **Gestione delle postazioni di lavoro** | Sono adottate misure per ridurre la possibilità che le postazioni di lavoro (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni, ecc.) vengano sfruttate per violare la sicurezza dei dati personali |
| **Utilizzo di infrastrutture sicure (hw e complementari)** | Le infrastrutture hardware e i sistemi complementari del CED sono oggetto di manutenzione periodica |
| **Infrastrutture logiche aggiornate** | Le infrastrutture software (es. middleware, software dei sistemi, ecc.) sono costantemente aggiornate |
| **Antivirus** | Sulle postazioni di lavoro sono installati antivirus aggiornati quotidianamente |
| **Network monitoring** | Si utilizzano strumenti di monitoraggio ed analisi del in transito, volti ad individuare situazioni anomale o malevoli |
| **Separazione LAN** | L'infrastruttura LAN del Data Center adotta la separazione tra ambienti sviluppo, test, collaudo e produzione |
| **Protezione della navigazione web (web filtering)** | Sulle postazioni di lavoro si utilizzano sistemi di web filtering per evitare l'accesso a risorse web non autorizzate |
| **Accessi da remoto con VPN** | Si utilizza il sistema/protocollo VPN per l'accesso alle risorse da remoto da parte di dipendenti e fornitori |
| **Protezione perimetrale (firewall)** | Vengono utilizzati strumenti di protezione della rete (Next Generation Firewall) per delimitare il perimetro di sicurezza del Data Center |
| **Protezione perimetrale di rete** | Vengono utilizzati strumenti di protezione degli attacchi DDoS |
| **Gestione Log accessi privilegiati (es. SIEM)** | Si utilizzano strumenti per la gestione dei log dei sistemi (es. log dei server dei database, dei firewall, ecc.). I log generati vengono esaminati e correlati per rilevare e gestire eventi di sicurezza (es. a fronte di un accesso illecito da un IP, si possono correlare i log degli apparati tracciati per esaminare cosa è avvenuto) |
| **Backup** | Sono adottati servizi infrastrutturali di backup |

Ulteriori misure tecniche di sicurezza implementate sul trattamento applicate dal Responsabile:

|  |  |
| --- | --- |
| **Misura** | **Descrizione/Esempi** |
| **Minimizzazione della quantità dei dati personali** | Nel trattamento sono adottate misure tecniche e/o di progetto per ridurre la quantità dei dati necessari quali tecniche di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, riduzione della natura identificativa del dato, riduzione dell'accumulazione, limitazione dell'accesso |
| **Sistema di autorizzazione** | Sono utilizzati sistemi di gestione delle autorizzazioni/ruoli applicativi che garantiscono che gli autorizzati accedano ai soli dati necessari per l’esecuzione delle attività assegnate |
| **Sistema di autenticazione** | Si utilizza un sistema di autenticazione (locale o nazionale) con un grado di sicurezza adeguato in relazione al trattamento |
| **Utilizzo di sistemi di autenticazione multifattore** | È previsto l'uso di certificati digitali, SPID o CIE per l'autenticazione dell'utente e/o per i servizi di cooperazione applicativa |
| **Gestione del ciclo di vita delle credenziali** | È garantita la gestione del provisioning delle credenziali di autenticazione (creazione, revoca, modifica di credenziali) e la gestione delle autorizzazioni/ruoli applicativi (attribuzione, aggiornamento o revoca del ruolo**)** |
| **Tracciabilità accessi risorse** | Vengono tracciati gli accessi alle risorse critiche impiegate nel trattamento (es database, front end e back end del servizio, share di rete). Il controllo può ad es. essere implementato per un database, andando a garantire la tracciatura dell'identificativo dell'utente che ha inserito/modificato/cancellato i dati della tabella |
| **Audit log applicativi** | L'applicazione software traccia mediante log operazioni significative compiute dagli utenti su dati personali. |
| **Abilitazioni puntuali accessi DB** | Ad ogni utente che accede a dati personali su database è assegnata una credenziale univoca (es. mediante utilizzo di proxy SQL) |
| **Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento** | Sono previste opportune tecniche per ridurre la vulnerabilità delle risorse impiegate nel trattamento (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali,) |
| **Pseudonimizzazione** | Sono adottate tecniche che garantiscono la non attribuzione di un dato a una persona identificata o identificabile ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato |
| **Cifratura del dato** | Sono adottati opportuni mezzi per cifrare i dati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.) |
| **cifratura del canale** | Viene utilizzato un canale cifrato per le comunicazioni mediante l'impiego di protocolli sicuri (es. HTTPS e SSH) nelle connessioni esposte all’esterno. |
| **Backup cifrati** | Sono utilizzati sistemi per la cifratura dei backup |
| **Protezione applicativa (WAF WEB Application Firewall)** | Vengono utilizzati strumenti di protezione dei Siti WEB Istituzionali degli applicativi WEB |
| **Disaster Recovery** | Sono adottate procedure per garantire il DR |
| **Business continuity** | Sono adottate procedure per garantire la BC |

**ALLEGATO 3**

**SCHEDA EVENTO DATA BREACH**

|  |  |
| --- | --- |
| **SCHEDA EVENTO** | |
| **CODICE** |  |
| Data evento e ora della violazione anche solo presunta (specificando se è presunta); |  |
| Data e ora in cui si è avuto conoscenza della violazione; |  |
| Fonte di segnalazione |  |
| Tipologia evento anomalo |  |
| Descrizione evento anomalo |  |
| Numero interessati coinvolti |  |
| Numerosità dei dati personali di cui si presume la violazione |  |
| Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza |  |
| Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili) |  |
| Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione |  |