**MODULO DI VALUTAZIONE DEI RESPONSABILI DEL TRATTAMENTO**

Al fine di garantire che le attività di trattamento di dati personali effettuate soddisfino i requisiti del Regolamento UE 2016/679 *(“General Data Protection Regulation”)*, nonché del D.Lgs. 196/03 per come modificato dal D.Lgs. 101/18, **Azienda Sanitaria Locale di Vercelli** (di seguito, semplicemente il *“titolare”*) ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate a tutelare i diritti e le libertà fondamentali dei soggetti interessati, ai sensi e per gli effetti dell’articolo 28, paragrafo 1, del suddetto Regolamento UE 2016/679.

Pertanto, Vi invitiamo a compilare il seguente modulo in ogni sua parte, in modo tale da poter valutare che le garanzie che la Vostra Organizzazione presenta, siano adeguate alla soddisfazione dei requisiti richiesti dalla normativa applicabile in materia di protezione dei dati personali, con particolare riferimento alle disposizioni in materia di sicurezza del trattamento.

In data 4 giugno 2021 la commissione UE 2021/915 ridefinisce le clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e

del Consiglio. (Testo rilevante ai fini del SEE)

Pertanto, ai sensi dell’articolo 28, paragrafo 3, lettera h), del Regolamento UE 2016/679, il titolare del trattamento si riserva altresì di verificare, in ogni momento, quanto di seguito dichiarato.

|  |  |
| --- | --- |
| **Titolare del trattamento** | **Azienda Sanitaria Locale di Vercelli** |
| **Responsabile del trattamento** |  |
| **Check list completata da** |  |
| **Checklist compilata in data** |  |

**SEZIONE A – DATI E MODALITÀ DEL TRATTAMENTO**

Come da nota esplicativa dell’Allegato III citato nella “DECISIONE DI ESECUZIONE”, si dichiara ***“Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente”, “Descrizione delle misure di sicurezza tecniche e organizzative messe in atto dal o dai responsabili del trattamento (comprese le eventuali certificazioni pertinenti) per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche”.***

**Riepilogo sezioni**

[SEZIONE A – DATI E MODALITÀ DEL TRATTAMENTO 2](#_Toc89423062)

[SEZIONE B – MISURE ORGANIZZATIVE 4](#_Toc89423063)

[SEZIONE C – MISURE TECNICHE 6](#_Toc89423064)

# **SEZIONE A – DATI E MODALITÀ DEL TRATTAMENTO**

|  |  |  |
| --- | --- | --- |
| **Domande** | | **Risposte** |
| **1** | Trattate per conto del titolare dati personali, oltre quelli indicati nell’accordo ex art. 28 e/o contratto? | Si  No |
| **2** | Trattate per conto del titolare dati personali di altre categorie di interessati, oltre quelle indicate nell’accordo ex art. 28 e/o contratto? | Si  No |
| **3** | I dati personali sono e/o saranno trattati - per conto del titolare - per finalità o scopi diversi da quelli indicati nell’accordo ex art. 28 e/o contratto? | Si  No |
| **4** | Ove applicabile, specificare le finalità o gli scopi diversi di cui alla domanda precedente. | Non applicabile  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | Quali sono le tipologie di dati trattati per conto del titolare? | Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **6** | Quali sono le modalità di trattamento dei dati? | Solo elettronica  Solo cartacea  Mista elettronica/cartacea |
| **7** | Specificare i luoghi (indicando anche dove si trovano i server, se presenti) dove il responsabile, gli autorizzati al trattamento e gli eventuali sub-responsabili trattano i dati personali per conto del titolare. | Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **8** | Precisare se l'hosting e gli ulteriori trattamenti dei dati personali effettuati per conto del titolare, sono limitati allo Spazio Economico Europeo (SEE). | Trattamenti eseguiti all’interno dello SEE  Trattamenti eseguiti anche all’esterno dello SEE, ed in particolare:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **9** | Nel caso in cui i dati personali siano trattati per conto del titolare al di fuori dello SEE, descrivere le misure di salvaguardia ai sensi degli artt. 46 e 47 GDPR per garantire che i dati siano adeguatamente protetti al di fuori dello SEE (per esempio: Clausole Contrattuali Standard Europee). | Non applicabile  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **10** | È stata effettuata la valutazione d’impatto sulla protezione dei dati (DPIA), nei casi in cui i servizi oggetto della fornitura presentino, per gli interessati, rischi elevati e/o uso di nuove tecnologie derivanti da utilizzi innovativi o applicazioni di nuove soluzioni tecnologiche od organizzative (riconoscimento biometrico, geolocalizzazione, etc.) e/o trattamenti di dati su larga scala e/o trattamenti di categorie particolari di dati personali? Se si, trasmettere al titolare tale documento. | Si  No  Non applicabile |

# **SEZIONE B – SICUREZZA - MISURE ORGANIZZATIVE**

|  |  |  |
| --- | --- | --- |
| **Domande** | | **Risposte** |
| **1** | Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti mediante lettera di incarico (ex art. 29 GDPR)? | Si  No |
| **2** | Tutte le persone autorizzate al trattamento partecipano, su base annuale, a corsi di formazione incentrati sugli obblighi previsti dalle normative vigenti in tema di protezione dei dati? | Si  No |
| **3** | Gli autorizzati coinvolti nel trattamento sono stati informati del dovuto obbligo si segretezza e riservatezza ai sensi dell’art. 2105 c.c. | Si  No |
| **4** | Avete adottato un registro delle attività di trattamento (ex art. 30 GDPR par. 2), in qualità di responsabile del trattamento? Se così fosse, ogni quanto tempo viene aggiornato? | Si  No  Aggiornato ogni:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | È stato nominato il Data Protection Officer (DPO), e quali sono i suoi dati di contatto? | Si  No  Dati di contatto:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **6** | Avete adottato misure organizzative interne volte a prevenire e gestire eventuali violazioni dei dati personali oggetto di trattamento (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)? Se si, elencare qui le evidenze fornite. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **7** | Avete un indirizzo e-mail o call center dedicato alla segnalazione di eventuali violazioni dei dati personali? | Si  No  Recapito:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **8** | Vi avvalete della collaborazione di sub-responsabili per la fornitura dei servizi offerti al titolare del trattamento? In caso affermativo, avete richiesto l'autorizzazione scritta al titolare del trattamento, prima di ricorrere a tali sub-responsabili per l’esecuzione delle attività di trattamento effettuate per conto dello stesso? Si prega di produrre l’elenco dei sub-responsabili, aggiornato alla data di compilazione della presente checklist. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **9** | Ogni sub-responsabile è tenuto a compilare questa checklist, sia al momento della sua autorizzazione, sia con cadenza annuale. Avete verificato (e verificate almeno una volta all'anno) l'adeguatezza delle misure tecniche e organizzative di ciascun sub-responsabile autorizzato, attraverso la presente checklist? | Si  No  Non applicabile |
| **10** | Ciascun sub-responsabile viene autorizzato sulla base di un atto il cui contenuto è sostanzialmente conforme a quello intercorrente tra il titolare ed il responsabile, relativamente ai doveri ed alle responsabilità del sub-responsabile? | Si  No  Non applicabile |
| **11** | Descrivere la procedura e soluzione adottata per il controllo degli accessi fisici | Non applicabile  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# **SEZIONE C – SICUREZZA - MISURE TECNICHE**

|  |  |  |
| --- | --- | --- |
| **Domande** | | **Risposte** |
| **1** | Disponete di certificazioni specifiche riferite alla sicurezza del trattamento dati e dati personali? | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **2** | Avete predisposto misure tecniche volte a prevenire il trattamento di dati personali per scopi diversi da quelli previsti dall’accordo al trattamento? | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **3** | Disponete di misure tecniche in grado di consentire la cancellazione, la rettifica, l'aggiornamento, la limitazione del trattamento e la portabilità dei dati personali su richiesta del titolare e/o al termine del contratto intercorrente con lo stesso? Si prega di descriverle o produrne documentazione. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **4** | Disponete di misure tecniche in grado di consentire la restituzione dei dati personali al titolare, su sua richiesta e/o al termine del contratto? Si prega di descriverle o produrne documentazione. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | Gli accessi delle persone autorizzate al trattamento ai sistemi IT sono protetti da ID e password personali? | Si  No |
| **6** | Sono state adottate policy relative alla gestione, rotazione, scadenza e blocco delle password per tutti i sistemi adottati e distribuiti? | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **7** | Disponete di un sistema per garantire la registrazione degli eventi? | Si  No |
| **8** | Le persone autorizzate al trattamento utilizzano account condivisi per accedere ai dati personali? | Si  No |
| **9** | È prevista una periodica revisione degli account?  (Account disabilitati, autorizzati dismessi, profili di autorizzazione cambiati. | Si  No  Cadenza di verifica in mesi: \_\_\_\_\_\_\_\_\_ |
| **10** | Disponete di misure tecniche che consentono l'accesso ai dati personali solo a sub-responsabili del trattamento autorizzati da apposito accordo o contratto di servizi? Si prega di descriverle o produrne documentazione. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **11** | Disponete di certificazione/garanzia di processi e prodotti | Si  No  Non applicabile |
| **12** | Avete adottato misure volte a ridurre al minimo il rischio che gli interessati siano identificati, e misure volte a mitigare gli effetti negativi per gli interessati in caso di violazione dei dati personali? (es. pseudonimizzazione, crittografia, visibilità dei dati personali limitata al solo set di informazioni necessario per le singole attività di elaborazione) | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **13** | Avete in atto una procedura di emergenza e di business continuity da seguire in caso di violazione dei dati personali? | Si  No  Allegare soluzione adottata  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **14** | È stata predisposta una procedura per l’eventuale di collaborazione con il Titolare del trattamento per l’esercizio dei diritti degli interessati previsti dagli artt.15-22 del GDPR? | Si  No  Non applicabile |
| **15** | Vengono distribuiti servizi tramite cloud? | Si  No  Dove sono situati i server: |
| **16** | Per quanto tempo vengono conservati i dati? | Periodo di conservazione, o criterio per stabilire tale periodo:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **17** | Disponete di misure di informatica interna e di gestione e governance della sicurezza informatica? | Si  No |
| **18** | Il sistema informativo è gli ambienti deputati al trattamento sono sottoposti, almeno una volta all'anno, a penetration test e/o vulnerability assessment? | Si  No |
| **19** | Avete in essere altre procedure tecniche che vengono regolarmente eseguite al fine di verificare l'adeguatezza delle misure di sicurezza volte a proteggere l'accesso ai dati personali? Si prega di descriverle o produrne documentazione. | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **20** | Tutti i supporti cartacei contenenti i dati personali sono conservati in armadi chiusi a chiave? | Si  No  Non applicabile |
| **21** | Sono state adottate misure e piani antincendio e anti allagamento dei locali in cui sono conservati i dati in formato cartaceo? | Si  No  Non applicabile |
| **22** | È stata adotta una procedura per la corretta distruzione e/o pulizia di: documenti cartacei e/o i supporti magnetici/ottici, hd di pc/server/NAS/DVR/NVR etc | Si  No |
| **23** | È stata valutata l’adozione dell’encryption in funzione dei dispositivi o dei data base? | Si  No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **24** | È prevista una policy aziendale che verifichi periodicamente le regole di accesso ai sistemi? (verifica regole firewall, VPN, Access point) | Si  No |
| **25** | I dati di produzione sono consentiti e limitati solo agli ambienti di produzione. In casi eccezionali e con le approvazioni necessarie, gli ambienti di test e di sviluppo possono elaborare dati personali (reali) nella misura in cui siano protetti come gli ambienti di produzione. Gli ambienti di test e di sviluppo, così come quelli di pre-produzione, utilizzano dati resi anonimi? | Si  No  Non applicabile |
| **26** | Proteggete i dati personali durante la trasmissione su reti aperte, pubbliche o non attendibili, con l’implementazione della strong cryptography o l’utilizzazione di protocolli sicuri? | Si  No |
| **27** | Sono utilizzati strumenti di sicurezza per monitorare e controllare il flusso di dati personali attraverso gli endpoint e verso le reti esterne? | Si  No |
| **28** | É stato adotta un sistema di logging degli access in qualità di AdS come da norma? | Si  No |
| **29** | In caso di fornitura di software e/o applicativi, viene garantita la conformità *privacy by design* prevista dall’art. 25 del GDPR? Indicare la conformità. | Si  No  Non applicabile |

***NOTE***

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

Il responsabile del trattamento

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

*(timbro e firma)*