

Allegato n. 4

**Oggetto: Adeguamento Regolamento Generale sulla Protezione dei Dati - UE 2016/679**

A seguito dell'applicazione del Regolamento generale per la protezione dei dati personali (*di seguito GDPR*), entrato in vigore il 25 maggio 2016 ed efficace dal 25 maggio, si porta alla Vostra attenzione quanto specificato nel testo del Regolamento, ed in particolare agli artt. 25, 32, 33, 34 e 35, recanti indicazioni in merito alla sicurezza dei dati personali.

Differentemente da quanto è previsto con il previgente Codice D.lgs. 196/2003, che individuava alcune misure minime di sicurezza, dettagliate nell'allegato B, il GDPR introduce il concetto di “...*misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio...*”, andando a definire un elenco non esaustivo di quanto dovrebbe essere applicato ad ogni singola attività di trattamento.

Il GDPR introduce il principio di *accountability* (tradotto in “*responsabilizzazione*”), ovvero la capacità di dimostrare di aver applicato ogni misura si ritenga utile e necessaria, al fine di garantire la sicurezza nelle attività di trattamento.

In quest'ottica quindi, non ci si limita più a valutare un livello “minimo” di sicurezza, ma si introducono vari elementi che impongono una valutazione sulle misure idonee a garantire un'adeguata sicurezza nelle attività di trattamento, tra le altre, se del caso:

- **Protezione dei dati fin dalla progettazione:** In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i fornitori dei prodotti, dei servizi e delle applicazioni dovrebbero tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati;
- **Protezione per impostazione predefinita:** garantire che l'attività di trattamento, per impostazione predefinita, avvenga solamente relativamente a dati personali necessari per ogni singola specifica finalità;
- **Pseudonimizzazione:** trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste siano conservate separatamente e soggette a misure tecniche e organizzative tali da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato;
- **Cifratura** dei dati personali, ovvero rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- **Capacità** di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- **Capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- **Procedure per testare**, verificare e valutare regolarmente l'**efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- Adesione a un **codice di condotta** di cui all'articolo 40 del GDPR;
- **Certificazione** nonché rilascio di sigilli e marchi di protezione dei dati, secondo quanto disposto all'articolo 42 del GDPR;
- **Sistemi di controllo** per evitare o arginare casi di violazione dei dati personali (data breach);

*Allegato n. 4*

- **Valutazione d'impatto sulla protezione dei dati**, secondo quanto previsto dall'art. 35 del GDPR, realizzata direttamente dal fornitore sul prodotto/servizio che va ad offrire;
- **Ogni ulteriore elemento ritenuto utile** dal fornitore per garantire un livello di sicurezza adeguato al rischio.

Il GDPR dispone inoltre che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato.

A tal motivo, dovranno anche essere fornite informazioni in merito ad eventuale trasferimento / trattamento dei dati con i Vs prodotti e/o servizi in paesi extra territorio UE, specificando i soggetti terzi coinvolti, i territori nei quali queste risiedono, ovvero dove sono dislocati i dati, e le garanzie applicate: si ricorda ad esempio che ricadono in questa analisi sistemi di storage in Cloud su server dislocati in territorio extra UE, oppure accesso da parte di altre società (*partecipate o controllate, partner, etc....*) ai prodotti / servizi da Voi offerti.

Relativamente ai servizi affidati in **Cloud** - IaaS, SaaS, PaaS- si devono poi proporre maggiori informazioni, sia sul fornitore che sul servizio stesso, con particolare riguardo a:

- Affidabilità del fornitore (*esperienza, capacità e affidabilità del fornitore; caratteristiche della connettività; qualificazione del personale impiegato*);
- Portabilità dei dati (*sono ovviamente privilegiati i servizi che lo favoriscono*);
- Garanzie sulla disponibilità e sulle prestazioni dei servizi in cloud (*garanzie sulla riservatezza e sulla continuità operativa*);
- Dislocazione dei server ed eventuali dipendenze da altri fornitori;
- Tempi e modalità di archiviazione e conservazione dei dati;
- Tutele legali (*responsabilità, compliance, legge applicabile, foro competente*).

Sul punto si richiamano le seguenti fonti:

- Gruppo di Lavoro art. 29 (WP29): Parere 05/2012 sul *cloud computing*, adottato il primo luglio 2012;
- Garante per la protezione dei dati personali: *Cloud computing* – La guida del Garante della Privacy per imprese e pubblica amministrazione (24 maggio 2012)
- Banca d'Italia: Circolare n. 263 del 27 dicembre 2006, 15° aggiornamento del 2 luglio 2015
- European Banking Authority: Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03, 20 dicembre 2017)
- Ulteriori numerosi documenti a cura dell'ENISA, della CONSIP e dell'AGID emanati nel tempo



Regione del Veneto

## Azienda ULSS n. 1 Dolomiti

PEC: [protocollo.aulss1@pecveneto.it](mailto:protocollo.aulss1@pecveneto.it)

Sede legale: via Feltre, n. 57 – 32100 – BELLUNO

Centralino Belluno: 0437 516111 Centralino Feltre: 0439 88311

Codice Fiscale e Partita IVA: 00300650256

**U.O.C. PROVVEDITORATO, ECONOMATO E GESTIONE DELLA LOGISTICA**

*Allegato n. 4*

Il sottoscritto \_\_\_\_\_, nato il \_\_\_\_\_, a \_\_\_\_\_

Legale rappresentante della Ditta \_\_\_\_\_

con la qualifica di (titolare, socio, procuratore, ecc.) \_\_\_\_\_ C.F. \_\_\_\_\_

**SEDE LEGALE** in \_\_\_\_\_ via \_\_\_\_\_

**PARTITA IVA** \_\_\_\_\_ **CODICE FISCALE** \_\_\_\_\_

Visto ed esaminato quanto sopra indicato, conformemente a quanto previsto dal Regolamento Generale sulla protezione dei dati - UE 2016/679,

**dichiara**

che la Ditta \_\_\_\_\_, ha adottato idonee misure atte a garantire un'adeguata sicurezza nelle attività di trattamento dei dati.

A tal fine produce la seguente documentazione attestante l'adeguatezza dei prodotti/servizi proposti:

- 1) *Schema di misure di sicurezza, redatto secondo metodologia ENISA.*
- 2) *Riportare l'eventuale ulteriore documentazione presentata..*
- 3) *..*

Data \_\_\_\_\_

\_\_\_\_\_   
 firma digitale del firmatario

Allegato n. 4

## MISURE TECNICHE ED ORGANIZZATIVE SECONDO LA METODOLOGIA ENISA

| CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA  | PRESENTE (SI/NO)<br><i>motivare la scelta, dettagliando ove possibile</i> |
|--|---|
| <b>Politica di sicurezza e procedure per la protezione dei dati personali</b>  |   |
| Viene documentata la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.   |   |
| <b>Ruoli e responsabilità</b>  |   |
| I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con le politiche di sicurezza.  |   |
| Per le attività che il fornitore, in qualità di responsabile del trattamento dei dati personali, effettua per conto del Titolare con il supporto di ulteriori sub fornitori, gli obblighi in materia di protezione dei dati sono imposti parimenti a questi - mediante contratto o altro atto giuridico – e l'elenco di tali soggetti è comunicata al Titolare, ed aggiornato ad ogni variazione.                                      |   |
| <b>Politica di controllo degli accessi</b>   |   |
| I diritti specifici di controllo degli accessi sono assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.   |   |
| <b>Gestione risorse/asset</b>  |   |
| L'organizzazione dispone di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro include almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). È stato assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT). |   |

*Allegato n. 4*

| CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA   | PRESENTE (SI/NO)<br><i>motivare la scelta, dettagliando ove possibile</i> |
|---|---|
| <b>Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT</b>  |   |
| L'organizzazione si assicura che tutte le modifiche alle risorse, agli apparati ed al sistema IT sono registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali delle modifiche apportate al sistema IT avviene con cadenza almeno annuale.   |   |
| Lo sviluppo software viene eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Se eseguito un test, vengono utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, sono previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.      |   |
| Sono previste e applicate alcune policy interne che disciplinano la gestione delle modifiche e che includono per lo meno: un processo che governa l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche è regolata con cadenza almeno annuale.               |   |
| <b>Gestione degli incidenti / Violazione dei dati personali (<i>Personal data breaches</i>)</b>   |   |
| È stato definito un piano di risposta agli incidenti ( <i>Incident Response Plan</i> ) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.   |   |
| <b>Obblighi di confidenzialità imposti al personale</b>   |   |
| L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di preassunzione e / o assunzione. |   |

*Allegato n. 4*

| CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA  | PRESENTE (SI/NO)<br><i>motivare la scelta, dettagliando ove possibile</i> |
|--|---|
| <b>Formazione</b>  |   |
| L'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali devono inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica. |   |
| <b>Generazione di file di log e monitoraggio</b>   |   |
| Vengono registrate le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.  |   |
| <b>Backup</b>  |   |
| Le copie dei backup vengono crittografate e archiviate in modo sicuro, anche offline.  |   |
| <b>Sicurezza del ciclo di vita delle applicazioni</b>  |   |
| Durante lo sviluppo del ciclo di vita vengono seguite le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.   |   |
| Specifici requisiti di sicurezza vengono definiti durante le prime fasi del ciclo di vita dello sviluppo.  |   |
| Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) vengono adottate in analogia con i requisiti di sicurezza.  |   |
| Vengono seguiti standard e pratiche di codifica sicure.  |   |
| Durante lo sviluppo, test e convalida viene eseguita l'implementazione dei requisiti di sicurezza iniziali.  |   |

*Allegato n. 4*

| CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA   | PRESENTE (SI/NO)<br><i>motivare la scelta, dettagliando ove possibile</i> |
|---|---|
| Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture vengono eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto. |   |
| Vengono eseguiti test periodici di penetrazione.  |   |
| Vengono ottenuti informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.  |   |
| I patch software vengono testati e valutati prima di essere installati in un ambiente operativo.  |   |
| <b>Sicurezza Fisica</b>   |   |
| Il perimetro fisico dell'infrastruttura del sistema IT non è accessibile da personale non autorizzato.  |   |
| Le zone sicure vengono definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi devono essere mantenuti e monitorati in modo sicuro.   |   |
| I sistemi di rilevamento antintrusione vengono installati in tutte le zone di sicurezza.  |   |
| Se del caso, vengono costruite barriere fisiche per impedire l'accesso fisico non autorizzato.  |   |
| Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) vengono attivati nella sala server.  |   |
| Il personale di servizio di supporto esterno ha accesso limitato alle aree protette.  |   |
| <b>Sicurezza su servizi in Cloud</b>  |   |
| Gli elementi di sicurezza richiesti dai fornitori di servizi in Cloud rispettano le indicazioni fornite da più fonti, in riferimento a:   |   |



Regione del Veneto

## Azienda ULSS n. 1 Dolomiti

PEC: [protocollo.aulss1@pecveneto.it](mailto:protocollo.aulss1@pecveneto.it)

Sede legale: via Feltre, n. 57 – 32100 – BELLUNO

Centralino Belluno: 0437 516111 Centralino Feltre: 0439 88311

Codice Fiscale e Partita IVA: 00300650256

**U.O.C. PROVVEDITORATO, ECONOMATO E GESTIONE DELLA LOGISTICA**

*Allegato n. 4*

| CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA   | PRESENTE (SI/NO)<br><i>motivare la scelta, dettagliando ove possibile</i> |
|---|---|
| <ul style="list-style-type: none"><li>- Affidabilità del fornitore (<i>esperienza, capacità e affidabilità del fornitore; caratteristiche della connettività; qualificazione del personale impiegato</i>);</li><li>- Portabilità dei dati (<i>sono ovviamente privilegiati i servizi che lo favoriscono</i>);</li><li>- Garanzie sulla disponibilità e sulle prestazioni dei servizi in cloud (<i>garanzie sulla riservatezza e sulla continuità operativa</i>);</li><li>- Dislocazione dei server ed eventuali dipendenze da altri fornitori;</li><li>- Tempi e modalità di archiviazione e conservazione dei dati;</li><li>- Tutele legali (<i>responsabilità, compliance, legge applicabile, foro competente</i>).</li></ul> |   |