**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, nonché del D.Lgs. 196/03 per come modificato dal D.Lgs. 101/18, il **Comune di Aprilia** (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.

Il presente questionario consente al Titolare di valutare che siano soddisfatti i requisiti relativi alla sicurezza del trattamento richiesti dalla normativa in materia di protezione dei dati personali.

**TRATTAMENTO** (compilata a cura del Titolare):

|  |  |  |
| --- | --- | --- |
| Descrizione e finalità del Trattamento | |  |
| Base giuridica del trattamento  (gli articoli richiamati come base giuridica fanno riferimento al Regolamento UE n. 679/2016) | |  |
| Categoria del trattamento | |  |
| Contitolare | |  |
| Responsabile esterno del Trattamento | |  |
| Altri destinatari compresi eventuali paesi terzi | |  |
| Natura dei dati personali | |  |
| Categorie Interessati | |  |
| Consenso degli interessati e modalità di acquisizione | |  |
| Tipologia del Trattamento | |  |
| Struttura di riferimento | |  |
| Durata del Trattamento | |  |
| **Titolare del trattamento** | Comune di Aprilia | |
| **Responsabile del trattamento** |  | |
| **Check list completata da** |  | |
| **Checklist compilata in data** |  | |

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

|  |  |  |
| --- | --- | --- |
| **Domande** | | **Risposte** |
| **1** | Quali sono le modalità di trattamento dei dati? | o Solo elettronica  o Solo cartacea  o Mista elettronica/cartacea |
| **2** | 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:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **3** | Precisare se l'hosting e gli ulteriori trattamenti dei dati personali effettuati per conto del titolare, sono limitati allo Spazio Economico Europeo (SEE). | o Trattamenti eseguiti all’interno dello SEE  o Trattamenti eseguiti anche all’esterno dello SEE, ed in particolare:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **4** | 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). | o Non applicabile  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | È stata effettuata la valutazione dei rischi per gli interessati derivanti dall’uso, da parte del titolare, dei servizi oggetto della fornitura in questione? | o Si  o No |
| **6** | 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. | o Si  o No  o Non applicabile |

**SEZIONE B – 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)? | o Si  o 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? | o Si  o No |
| **3** | Avete adottato un registro delle attività di trattamento (ex art. 30 GDPR), in qualità di responsabile del trattamento? Se così fosse, ogni quanto tempo viene aggiornato? | o Si  o No  Aggiornato ogni:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **4** | È stato nominato il Data Protection Officer (DPO), e quali sono i suoi dati di contatto? | o Si  o No  Dati di contatto:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | 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. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **6** | Avete un indirizzo e-mail o call center dedicato dove possono essere segnalate eventuali violazioni dei dati personali? | o Si  o No  Recapito:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **7** | Avete dei 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. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **8** | 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? | o Si  o No  o Non applicabile |
| **9** | 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? | o Si  o No  o Non applicabile |

**SEZIONE C – MISURE TECNICHE**

|  |  |  |
| --- | --- | --- |
| **Domande** | | **Risposte** |
| **1** | Disponete di misure tecniche per garantire un adeguato livello di sicurezza all'interno dei sistemi IT utilizzati nel trattamento di dati personali effettuato per conto del titolare? Si prega di descriverle o produrne documentazione. | o Si  o 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? (es. i dati personali non devono poter essere copiati su supporti rimovibili, ad eccezione dei supporti espressamente autorizzati dal responsabile per attività specifiche) | o Si  o 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. | o Si  o 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. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **5** | Gli accessi delle persone autorizzate al trattamento ai sistemi IT sono protetti da ID e password personali? | o Si  o No |
| **6** | La password che ogni autorizzato al trattamento utilizza per accedere ai sistemi IT è formata da almeno 8 caratteri, non facilmente riferibile all’autorizzato (cioè diversa dalla sua password di accesso) e modificata quando usata per la prima volta e ogni 3 mesi? | o Si  o No |
| **7** | Laddove la tipologia dei dati trattati lo richieda, è previsto il cambio della password ogni 3 o 6 mesi? | o Si  o No  o Non applicabile |
| **8** | Le persone autorizzate al trattamento utilizzano account condivisi per accedere ai dati personali? | o Si  o No |
| **9** | Disattivate le credenziali di autenticazione che non vengono utilizzate da almeno 6 mesi? | o Si  o No |
| **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. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **11** | I profili di accesso ai sistemi IT vengono riesaminati almeno una volta all'anno per verificare che siano corretti, secondo un principio di profilazione degli accessi che tenga conto del ruolo e delle responsabilità di ciascun utente/autorizzato al trattamento? | o Si  o No |
| **12** | Le credenziali di accesso sono disattivate quando l’autorizzato al trattamento non ha più diritto di accedere ai dati personali (ad esempio, per cessazione del rapporto di lavoro o cambio di mansione)? | o Si  o No |
| **13** | Gli accessi amministrativi individuali da remoto ai sistemi che gestiscono i dati personali sono protetti mediante un meccanismo di autenticazione che richiede modifica della password ogni 90 giorni? Si consiglia di dotarsi di strumenti per la gestione delle password (tool ad hoc), per garantire la sicurezza delle credenziali. | o Si  o No  o Non applicabile |
| **14** | L'accesso da remoto (da reti esterne) agli ambienti che trattano dati personali è protetto mediante autenticazione a più fattori? | o Si  o No  o Non applicabile |
| **15** | 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) | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **16** | Avete in atto una procedura di emergenza e di business continuity da seguire in caso di violazione dei dati personali? | o Si  o No |
| **17** | È stata predisposta una procedura per l’esercizio dei diritti degli interessati previsti dagli artt.15-22 del GDPR? | o Si  o No |
| **18** | Vengono utilizzati servizi in cloud? | o Si  o No |
| **19** | Per quanto tempo vengono conservati i dati? | Periodo di conservazione, o criterio per stabilire tale periodo:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **20** | È stato predisposto un sistema di backup? | o Si  o No |
| **21** | Il backup dei dati personali è eseguito almeno una volta alla settimana? | o Si  o No  o Non applicabile |
| **22** | È stata predisposta una procedura di disaster recovery? | o Si  o No |
| **23** | I sistemi antivirus e firewall sono aggiornati almeno una volta al mese? | o Si  o No |
| **24** | I sistemi IT mediante i quali vengono trattati i dati personali sono sottoposti, almeno una volta all'anno, a penetration test e/o vulnerability assessment? | o Si  o No |
| **25** | 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. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **26** | Adottate sistemi di avviso in caso di trasferimento di grandi quantità di dati personali, violazioni dei dati personali o attacchi informatici (come DDoS - Distributed Denial of Service)? | o Si  o No |
| **27** | Tutti i supporti cartacei contenenti i dati personali sono conservati in armadi chiusi a chiave? | o Si  o No  o Non applicabile |
| **28** | È stato predisposto un sistema di archiviazione e conservazione della documentazione cartacea in luogo chiuso e non accessibile al pubblico? | o Si  o No  o Non applicabile |
| **29** | L'accesso ai luoghi in cui vengono conservati i dati personali viene controllato tramite un sistema di badge o qualsiasi altra forma di controllo? Si prega di specificare il sistema di controllo degli accessi. | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **30** | I documenti cartacei e/o i supporti magnetici/ottici (ad es. dischi rigidi, DVD, CD, smart card, chiavette USB) vengono distrutti o resi inutilizzabili per garantire che i dati e le informazioni in essi contenuti non possano essere ricostruiti e/o utilizzati (anche parzialmente) da terze parti non autorizzate? | o Si  o No |
| **31** | I documenti cartacei vengono fisicamente distrutti prima di essere cestinati attraverso dispositivi specifici quali distruggi documenti? | o Si  o No |
| **32** | Sono state adottate misure e piani antincendio e anti allagamento dei locali in cui sono conservati i dati in formato cartaceo? | o Si  o No  o Non applicabile |
| **33** | Avete adottato misure volte a prevenire la lettura, la copia, la modifica o la cancellazione non autorizzate di dati personali durante il loro eventuale trasferimento o durante il trasporto di supporti contenenti i dati? | o Si  o No |
| **34** | L’archiviazione di database/archivi di dati è basata su una classificazione appropriata degli asset, in base al livello di criticità? Ad esempio, i database/data storage che vengono utilizzati per la memorizzazione di una grande quantità di dati personali sono protetti tramite strong encryption? In caso affermativo, quale granularità è applicata? | o Si  o No  Evidenze fornite:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **35** | Per la dismissione degli asset IT sono messe in atto procedure di pulizia sicura al fine di rimuovere tutti i dati personali e/o sovrascrivere in modo sicuro prima dello smaltimento o del riutilizzo dello strumento? | o Si  o No |
| **36** | Firewall e router sono configurati al fine di limitare il traffico, in entrata e in uscita, da reti "non attendibili" (inclusi wireless) e sistemi? | o Si  o No |
| **37** | È negato tutto il resto del traffico, ad eccezione dei protocolli necessari all’ambiente che tratta dati personali? | o Si  o No |
| **38** | I firewall delle applicazioni sono configurati davanti ai server web appartenenti all’ambiente che tratta dati personali, al fine di verificare e convalidare il traffico che è diretto al server? | o Si  o No |
| **39** | Qualsiasi servizio o traffico non autorizzato viene bloccato e viene generato un avviso? | o Si  o No |
| **40** | 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? | o Si  o No  o Non applicabile |
| **41** | 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? | o Si  o No |
| **42** | Sono utilizzati strumenti di sicurezza per monitorare e controllare il flusso di dati personali attraverso gli endpoint e verso le reti esterne? | o Si  o No |
| **43** | L'accesso agli ambienti di produzione contenenti dati personali, ed in generale l'accesso ai sistemi contenenti dati personali del titolare del trattamento, sono monitorati e loggati al fine di tracciare l'accesso dell'utente Amministratore di Sistema (AdS) che accede ai dati personali? Si precisa che, in caso di necessità e/o di prescrizione normativa, il titolare del trattamento dei dati personali ha il diritto di ottenere i log dai responsabili del trattamento e/o da eventuali sub-responsabili. | o Si  o No  o Non applicabile |
| **44** | Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al rispetto della normativa? | o Si  o No |
| **45** | Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi? | o Si  o No |
| **46** | Sono stati comunicati al titolare del trattamento i nominativi degli AdS eventualmente individuati ed autorizzati dal responsabile? | o Si  o No  o Non applicabile |
| **47** | 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. | o Si  o No  o Non applicabile |

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.

Il responsabile del trattamento

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

*(timbro e firma)*