ALLEGATO III

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei trattamenti e dei dati

NOTA ESPLICATIVA: le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente e devono deve prendere anche le specifiche misure adottate al fine di fornire assistenza al Titolare del trattamento. Le misure si devono riferire alla specifica fattispecie – eliminare le misure non pertinenti e non applicabili e eventualmente aggiungere misure non previste.

Si descrivono di seguito le misure di sicurezza tecniche e organizzative che il Responsabile del trattamento deve mettere in atto, (comprese le eventuali certificazioni in possesso del Responsabile del trattamento pertinenti, ove presenti), 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.

1) *PRIVACY BY DESIGN E BY DEFAULT*:

Il Responsabile del trattamento deve rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e protezione dei dati per impostazione predefinita (*privacy by default*) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate ed adottate per rispettare tali principi (cfr. Considerando 78 GDPR).
In attuazione di tali principi, il Responsabile del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, dovrà eseguire un'analisi dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica e non sono compatibili con le finalità del trattamento previste dal Titolare, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento unionale e nazionale.

2) ELENCO AGGIORNATO SUB-RESPONSABILI:
Quando il primo Responsabile del trattamento è autorizzato a ricorrere a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, a prescindere dal carattere specifico o generale dell'autorizzazione preliminare scritta del Titolare del trattamento, il primo Responsabile deve tenere un elenco aggiornato degli altri (sub-)responsabili. Su richiesta del Titolare e/o e in caso di accertamenti anche da parte del Garante, il primo Responsabile del trattamento gli fornisce prontamente e non oltre 24 ore copia dell'elenco aggiornato.
Il Primo Responsabile del trattamento si impegna a fornire in modo proattivo al titolare del trattamento tutte le informazioni sull'identità (ad esempio nome, indirizzo, persona di contatto) di tutti i sub-responsabili del trattamento, e a tenerle sempre aggiornate.

3) ATTIVITA' DI REVISIONE, COMPRESE LE ISPEZIONI:

Su richiesta del Titolare del trattamento, a intervalli annuali o se vi sono indicazioni di inosservanza, il Responsabile del trattamento consentirà e contribuirà alle attività di revisione delle attività di trattamento di cui alle presenti clausole. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento potrà tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento.
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 di almeno 72 ore.

4) TRASFERIMENTO DATI EXTRA UE:

È generalmente vietato qualunque trasferimento di dati da parte del Responsabile del trattamento verso un paese terzo o un'organizzazione internazionale, ovvero a sub-responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale del GDPR, compresi trasferimenti successivi.
Il Responsabile del trattamento si assicura che anche il sub-Responsabile del trattamento non effettui trasferimenti di dati verso un paese terzo o un'organizzazione internazionale.
Il Primo Responsabile, nella scelta di ulteriori fornitori, deve privilegiare, a parità di garanzie in materia di protezione dei dati personali, fornitori che sono situati sul territorio nazionale e dell'Unione europea, istruendoli sulla necessità di conservare i dati all'interno dell'Unione stessa.
In presenza di una decisione di adeguatezza (cfr. https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero), il Primo Responsabile del trattamento è tenuto in ogni caso a chiedere specifica autorizzazione al Titolare, in considerazione degli obblighi connessi ai trasferimenti internazionali di cui al capo V del GDPR.
In via del tutto residuale, il Primo Responsabile può ricorrere a responsabili situati in Paesi terzi, richiedendo, ove possibile, l'implementazione di misure supplementari al fine di impedire l'identificazione dell'interessato da parte del responsabile e/o da autorità governative straniere.
In generale, quindi, il Primo Responsabile è in ogni caso tenuto a rispettare le misure previste dal capo V del GDPR, ponendo in essere le misure contrattuali necessarie anche per conto di ulteriori Sub-Responsabili. Ad ogni modo, il trasferimento di dati extra UE può essere 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 GDPR (cfr. https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=it&uri=CELEX%3A32021D0914).

5) AMMINISTRATORE DI SISTEMA:

Nel caso in cui il Responsabile effettua trattamenti, anche in parte, mediante strumenti elettronici, si impegna ad individuare e a designare gli Amministratori di Sistema ("AdS"), conformandosi altresì, nell'affidamento di tale incarico, a tutto quanto previsto dal provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009.
Le persone fisiche designate AdS considerate come tali sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Delle misure e degli accorgimenti prescritti con la designazione di Amministratore di Sistema il Responsabile del trattamento è tenuto a darne la prova; deve altresì conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, tenendo costantemente aggiornato tale documento interno (come da Allegato V) e in caso di accertamenti anche da parte del Garante fornire prontamente e comunque entro 24 ore il medesimo documento al Titolare.

6) MISURE MINIME:

Il Responsabile deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici.
Per il tramite degli Amministratori di Sistema designati, si impegna a garantire di default le modalità tecniche più efficaci per garantire un livello di sicurezza adeguato al rischio per la sicurezza dei dati.
Il Responsabile si impegna ad installare e mantenere aggiornate, sugli strumenti elettronici oggetto del contratto, tutte le misure e gli accorgimenti eventualmente prescritti dai Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali (GPDP), dall'Agenzia per l'Italia Digitale

(AGID) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), applicabili al servizio commissionato, nonché le ulteriori misure di sicurezza previste nel contratto di fornitura.
Nello specifico, il Responsabile si impegna al rispetto e alla dimostrazione di quanto previsto da:

- le Linee guida - Sicurezza nel Procurement ICT (Pubblicato il 19/05/2020 - Aggiornato il 19/05/2020) e disponibile anche alla seguente url: https://trasparenza.agid.gov.it/download/4514.html
- Linee guida per lo sviluppo del software sicuro (Ultimo aggiornamento 06-05-2020), disponibile alla seguente url: https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
- le «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (G.U Serie Generale n.103 del 05-05-2017), disponibili anche alla seguente url: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- Linee guida ACN rafforzamento resilienza (novembre 2024), disponibili anche alla seguente url: https://www.acn.gov.it/portale/documents/20119/564002/Linee+guida+ACN+rafforzamento+resilienza.pdf/d143d555-eeb0-766b-8e50-46f5f3012bd9?t=1736781799873

In ogni caso, il Responsabile è tenuto a fare tutto quanto è possibile per evitare la violazione di dati, in primo luogo adottando costantemente le misure di mitigazione che sono pubblicamente diffuse, specialmente quelle raccomandate dall'ACN.

- Sui criteri per l'approvvigionamento di beni e servizi affinché tengano conto degli elementi di cybersicurezza si veda l'art. 14 della L. 90/2024.

7) MISURE ULTERIORI:

NOTA ESPLICATIVA: adattare alla singola fattispecie – eliminare le misure non pertinenti e non applicabili

Il Responsabile del trattamento, ferma la dimostrazione della loro adozione, si impegna a mettere in atto misure tecniche e organizzative più specifiche, come di seguito:

a) mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento.

a.1) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;

a.2) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che l'autenticazione dei soggetti autorizzati avvenga tramite un processo di autenticazione multifattoriale (MFA);

a.3) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione;

a.4) crittografia dei dati che i dispositivi del fornitore/Responsabile (computer, portatili, tablet, ecc.) devono rispettare;

a.5) l'accesso alla rete locale dell'amministrazione da parte del fornitore/Responsabile deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit;

a.6) nelle forniture di sviluppo e manutenzione, l'utilizzo dei dati dell'amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su

server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Tale misura consiste nel gestire l'accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi.

b) mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
c) rilevare e detenere a norma di legge copia dei log di accesso all'applicativo e di sistema;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
e) nomina di un DPO, nei casi previsti dall'art. 37 GDPR ovvero per i soggetti privati obbligati alla sua designazione. Nel caso in cui il Responsabile del trattamento ritenesse tale nomina non obbligatoria, alla luce del principio di accountability è tenuto a dare la prova della mancanza dei criteri di nomina (cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, punto nn. 3 e 4);
f) poter dimostrare che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione;
g) una procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (cd. "Data Breach");
h) sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del GDPR con massimali adeguati;
i) il Responsabile è tenuto ad effettuare preliminarmente, e indipendentemente dal titolare del trattamento, una Valutazione del Rischio per la sicurezza dei dati (v. ad es.: https://www.enisa.europa.eu/risk-level-tool/risk) che tenga in considerazione i rischi presentati dal trattamento come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati (cfr. considerando 83 GDPR);
l) Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise);
m) Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati;
n) Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
o) Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE;
p) laddove la tipologia del trattamento rientri nell'elenco di cui all'ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018), il Responsabile è tenuto ad effettuare preliminarmente, e indipendentemente dal titolare del trattamento, una Valutazione d'impatto sul prodotto/servizio (cfr. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8581268).

7.1) Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto, il Titolare verifica che il fornitore/Responsabile rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate.
- "libretto di manutenzione" del prodotto (software o hardware), con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato.

  In particolare, nel libretto di manutenzione deve essere indicato:

- produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
- indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
- indicazioni sul processo di installazione degli aggiornamenti sicurezza;
- documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza);

7.2) Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l'hardware dismesso venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull'hardware dismesso stesso.
Nei rapporti contrattuali col Responsabile va definito un processo di verifica strutturato che deve almeno prevedere:

- la consegna di un verbale di avvenuta distruzione da parte del fornitore;
- nel caso di sistemi critici, la programmazione di una azione ispettiva o di altri sistemi di monitoraggio e/o controllo.

7.3) Manutenzione - aggiornamento dei prodotti:

E' fatto obbligo agli amministratori di sistema di eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

7.4) Vulnerability Assessment

Il Fornitore/Responsabile deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment a cadenza almeno annuale, e ogniqualvolta si apportano modifiche alla configurazione software/hardware.
Ad ogni modo, il Primo Responsabile e gli eventuali Sub-Responsabili sono chiamati a implementare le misure di sicurezza sopra indicate, ferma restando la necessaria predisposizione di ogni misura tecnica e organizzativa adeguata a garantire un livello di sicurezza adeguato al rischio, ai sensi degli artt. 5, parr. 1, lett. f), e 2, e 32 del GDPR. In ossequio ai principi di privacy by design e by default e con riferimento alla natura, al contesto e ai trattamenti connessi ai trattamenti effettuati, il Primo Responsabile e gli eventuali Sub-Responsabili possono concordare misure tecniche e organizzative aggiuntive rispetto a quanto previsto nel presente contratto.

7.5) Altre misure tecniche e organizzative:

NOTA ESPLICATIVA: eliminare quelle non pertinenti e aggiungere quelle mancanti:

- misure di pseudonimizzazione e cifratura dei dati personali;
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- misure per assicurare la 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
- misure di identificazione e autorizzazione dell'utente misure di protezione dei dati durante la trasmissione misure di protezione dei dati durante la conservazione

- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati misure per garantire la registrazione degli eventi
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita misure di informatica interna e di gestione e governance della sicurezza informatica
- misure di certificazione/garanzia di processi e prodotti misure per garantire la minimizzazione dei dati misure per garantire la qualità dei dati
- misure per garantire la conservazione limitata dei dati misure per garantire la Responsabilità
- misure per consentire la portabilità dei dati e garantire la cancellazione]

8) PERSONALE AUTORIZZATO:

Il Responsabile del trattamento si impegna a produrre ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art. 29 del GDPR. Inoltre, il Responsabile s'impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre, deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e la gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.
Considerato che il rispetto delle disposizioni contenute nelle regole deontologiche, ai sensi dell'art. 2-quater del D.lgs. n. 196/2003, come novellato dal D.lgs. 101/2018, costituisce per il Titolare del trattamento condizione essenziale per la liceità e la correttezza del trattamento dei dati personali, quest'ultimo obbliga il Responsabile del trattamento affinché anche il proprio personale autorizzato sia impegnato al rispetto delle seguenti:

☐ Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica (G.U. del 4 gennaio 2019, n. 3);

☐ Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica (G.U. del 14 gennaio 2019, n. 11);

☐ Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (G.U. del 14 gennaio 2019, n. 11);

☐ Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria (G.U. del 15 gennaio 2019, n. 12);

☐ Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica (G.U. del 15 gennaio 2019, n. 12);

☐ nessuna delle Regole deontologiche di cui supra.

9) REGISTRO DEL TRATTAMENTO:

Il Responsabile del trattamento, anche laddove non rientri nelle casistiche definite dall'art. 30, parr. 2 e 5, del GDPR tiene per iscritto un Registro delle attività relative ai trattamenti svolti per conto del Titolare.

10) ASSISTENZA AL TITOLARE:

In generale, il Responsabile del trattamento è tenuto ad assistere il Titolare nel garantire il rispetto degli obblighi a cui è vincolato quest'ultimo e a rispondere prontamente e comunque non oltre 72 ore dalle richieste di informazioni del Titolare del trattamento.
Il Responsabile comunicherà ogni informazione utile al fine di assistere il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti. Qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti, informa senza indugio e comunque non oltre 72 ore il Titolare affinché possa garantire che i dati personali siano esatti e aggiornati.
Nel caso in cui riceva richieste degli interessati per l'esercizio dei loro diritti, il Responsabile notifica prontamente e comunque non oltre 72 ore al Titolare del trattamento qualunque richiesta ricevuta dall'interessato in quanto non è autorizzato a rispondere egli stesso alla richiesta.
Inoltre, il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del GDPR, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi adottate in conformità all'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti per garantire un livello di sicurezza adeguato al rischio.
Il Responsabile si impegna a predisporre, condividere e aggiornare periodicamente la valutazione del rischio per la sicurezza dei dati e la valutazione di impatto sulla protezione dei dati e, comunque, a redigere uno o più atti di documentazione delle scelte, dando atto della conformità alla normativa sulla protezione delle persone con riguardo al trattamento dei dati e alla circolazione dei dati, ovvero indicando che il trattamento presenterebbe un rischio elevato.
Laddove la valutazione di impatto sulla protezione dei dati presentasse un rischio elevato, anche in fase di consultazione con la/le autorità di controllo competenti, il Responsabile assisterà il Titolare del trattamento per adottare le misure adeguate per attenuare il rischio.
Il Responsabile si impegna ad adibire apposito ufficio/referente, segnalando un punto di contatto diretto al Titolare del trattamento, alle incombenze relative alla notificazione e comunicazioni previste dal GDPR.

11) COMUNICAZIONE E REGISTRO DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DI DATI PERSONALI

In caso di incidente di sicurezza e/o di violazione dei dati personali (cd. Data Breach), senza indugio il Responsabile del trattamento coopera con il Titolare e lo assiste nell'adempimento degli obblighi, ai sensi degli artt. 33 e 34 GDPR.
Nel caso di incidente di sicurezza e/o di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà comunicazione al Titolare senza ingiustificato ritardo e comunque non oltre 24 ore dopo esserne venuto a conoscenza. La comunicazione iniziale contiene le informazioni disponibili in quel momento e le altre informazioni sono fornite non appena disponibili, senza ingiustificato ritardo. Il Responsabile documenta qualsiasi incidente di sicurezza e/o di violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Il Responsabile deve mantenere un Registro degli incidenti di sicurezza, anche qualora non vi siano delle violazioni dei dati personali, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.

A seguito del verificarsi di detti incidenti il Titolare potrà:

- effettuare le succitate attività di revisione, comprese le ispezioni;

- prescrivere l'adozione di misure di sicurezza aggiornate e/o ulteriori anche rispetto a quelle previste dal presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto (cfr. la succitata Clausola 10).

Il Responsabile deve adottare procedure tecniche e organizzative volte alla gestione di eventuali incidenti di sicurezza e di violazioni di dati personali; deve disporre altresì di una struttura per la prevenzione e gestione degli incidenti informatici e delle violazioni di dati personali con il compito d'interfacciarsi con le analoghe strutture del Titolare.

12) LINEE GUIDA E PROVVEDIMENTI DELL'AUTORITA' GARANTE PRIVACY:

NOTA ESPLICATIVA: eliminare i provvedimenti non pertinenti e aggiungere quelli applicabili alla fattispecie ove esistenti:

Il Responsabile del trattamento s'impegna a mettere in atto le misure tecniche e organizzative previste da Linee Guida e provvedimenti adottati dalle Autorità europee in materia di protezione dei dati personali, con particolare riferimento a quelli adottati dal Garante Privacy italiano quali:

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 ((Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015);
- Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Posta elettronica e internet – 1° marzo 2007;

_____

- *Altro*

In materia di protezione di dati personali il Responsabile del trattamento si impegna a rispettare e mettere in atto, vigilando sulla loro applicazione, le misure previste nei codocumenti che seguono:

☐ Allegato A: Misure tecniche e organizzative applicate dalle SWH per garantire i requisiti di Privacy by Design e by Default nelle Attività di sviluppo dei Software Gestionali, di cui al CODICE DI CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO DALLE IMPRESE DI SVILUPPO E PRODUZIONE DI SOFTWARE GESTIONALE (Pubblicato sulla Gazzetta Ufficiale Serie Generale del 278 del 27 novembre 2024) VEDI ANCHE PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI N. 618 DEL 17 OTTOBRE 2024

☐ Allegato B: Misure di sicurezza applicate dalle SWH per lo svolgimento dei Servizi riguardanti i SW Gestionali impiegati nei contesti on premise e in cloud, di cui al CODICE DI CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO DALLE IMPRESE DI SVILUPPO E PRODUZIONE DI SOFTWARE GESTIONALE (Pubblicato sulla Gazzetta Ufficiale Serie Generale del 278 del 27 novembre 2024) VEDI ANCHE PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI N. 618 DEL 17 OTTOBRE 2024

☐ Linee guida in materia di conservazione delle password (ACN & GPDP, Provvedimento n. 594 del 7 dicembre 2023, come peraltro prescritto dall'art. 9 della L. n. 90/2024)

☐ Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021

☐ Provvedimento in materia di videosorveglianza - 8 aprile 2010;
☐ Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
☐ RFID Etichette intelligenti: prescrizioni - 9 Marzo 2005;
☐ Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
☐ Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
☐ Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute 15 maggio 2013;
☐ Trattamento di dati personali per profilazione on line - 19 marzo 2015;
☐ Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di *mobile remote payment* – 22 maggio 2014 *(Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014)*
☐ Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15 maggio 2014;
☐ Dossier sanitario - 4 giugno 2015
☐ Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;
☐ Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica
☐ per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.
☐ Le buone prassi in materia di sicurezza o Privacy proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione);
☐ Le buone prassi in materia di sicurezza o Privacy proposte da associazioni:
(*Esempio:*
- *Center for Internet Security;*
- *Critical Security Controls for Effective Cyber Defense;*
- *CIS Benchmarks;*
- *Altro)*

☐ *Altro*_____

13) CERTIFICAZIONI PERTINENTI:

Per attestare l'adeguatezza delle misure di sicurezza adottate (cfr. art. 28.5 del GDPR), il Responsabile del trattamento aderisce a specifici codici di condotta o a schemi di certificazione come di seguito:

NOTA ESPLICATIVA: valorizzare le certificazioni possedute ed eliminare quelle non pertinenti.

a) visto l'art. 43.1.b) del GDPR, che prevede una certificazione accreditata IS0 17065, il Responsabile del trattamento ha ottenuto il rilascio delle seguenti certificazioni:

[ ] ISDP©10003 (ITA);
[ ] Carpa (LU);
[ ] Europrivacy (LU);
[ ] Europrice (D);
[ ] altra certificazione accreditata IS0 17065 in materia di protezione dei dati personali;

b) visto l'art. 32 (nonché l'art. 25) del GDPR, anche se la norma di accreditamento ISO 17021-1 non è da considerarsi valida ai fini del GDPR, pur tuttavia molti argomenti trattati hanno riscontro in specifici requisiti di legge europei e nazionali, il Responsabile del trattamento possiede le seguenti certificazioni, con il relativo ambito di applicazione:

[ ] ISO/IEC 27001 [indicare l'ambito di applicazione];
[ ] ISO/IEC 22301;
[ ] ISO/IEC 20000-1;
[ ] ISO/IEC 27701;
[ ] ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001;
[ ] altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni;

c) il Responsabile del trattamento ha ottenuto inoltre le seguenti certificazioni:

[ ] ISO 9001;
[ ] ISO 13485;
[ ] altra certificazione accreditata in materia di gestione della qualità;

[ ] *ALTRO*_____.

d) visto l'art. 106, comma 8, del D. Lgs. n. 36/2023, "*Garanzie per la partecipazione alla procedura*", ai fini del presente affidamento il Responsabile del trattamento ha ottenuto tra le norme di certificazione ivi previste le seguenti:

[ ] *ALTRO*_____.

14) INFORMAZIONI SUL TRATTAMENTO E CONSENSO DELL"INTERESSATO:

Nel caso in cui il/i trattamenti oggetto del presente contratto si basino sul consenso l'informativa redatta dal Titolare del trattamento deve essere:
☐ Consegnata a mano all'interessato;
☐ Pubblicata online sul sito XXXX;
☐ Non applicabile;
☐ Consegnata dal Titolare stesso;
☐ *Altro (specificare nello spazio sottostante).*

Gestione del consenso.

Quando il trattamento si fonda sulla base giuridica del consenso "libero" dell'interessato viene fornita dal Titolare specifica informativa e viene richiesto apposito consenso in mancanza del quale non si procederà al relativo trattamento.
Il consenso va raccolto e registrato tramite:
☐ Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare del trattamento;
☐ Informativa e modulo raccolta consenso cartaceo redatto a cura del Titolare e reso/raccolto da XXXX che dovrà consegnare la modulistica firmata al Titolare del trattamento;

☐ Raccolta e registrazione del consenso tramite sistema informatico XXXX;
☐ Altro;
☐ Non applicabile.