Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

AL26

PROCEDURA INTERNA SUL RISPETTO DEI PRINCIPI DI "PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE" (PRIVACY BY DESIGN) E DI "PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA" (PRIVACY BY DEFAULT)

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE, (P. IVA: 09323530965) (infra "ASST RHODENSE"), in persona del suo legale rappresentante pro tempore, con sede legale in Garbagnate Milanese (MI), viale Forlanini, 95, intende illustrare, di seguito, il principale contenuto (e scopo) dei (fondamentali) principi di "privacy by design" e di "privacy by default" ex art. 25[1] e Considerando n. 78)[2] del GDPR, da tenere a mente (e, di conseguenza, da rispettare) ad opera di ogni soggetto ex artt. 4 n. 10), 29 e 32 paragrafo 4) del GDPR autorizzato al trattamento dei dati personali da parte di ASST RHODENSE medesima, la quale agisce, in via principale, nella veste di Titolare (o Responsabile) del trattamento, e soltanto in specifiche e particolari ipotesi come co-Titolare e/o sub-Responsabile del trattamento.

1. Premesse.

1.1. L'adesione ai principi di "**privacy by design**" (ossia, protezione dei dati sin dalla progettazione) e di "**privacy by default**" (ossia, protezione dei dati per impostazione predefinita) rappresenta un onere, passibile di sanzione (amministrativa) ex art. 83 paragrafo 4) lettera a) del GDPR, in capo a ciascun Titolare (e/o Responsabile) del trattamento, indipendentemente dalle proprie dimensioni (societarie) ovvero dalla complessità del trattamento posto in essere (o da porre in essere).

Nello specifico, essi rappresentano concetti tra loro complementari, ed idonei a rafforzarsi a vicenda: infatti, il Titolare (o il Responsabile) del trattamento deve **prenderli in considerazione sin dal momento iniziale in cui viene pianificata una nuova operazione di trattamento**[3], **nei riguardi di quelle attività di trattamento già intraprese prima dell'entrata in vigore del GDPR (e continuate dopo la sua diretta applicabilità all'interno dei Paesi Membri dell'UE), e, infine, deve tenerli a mente (e, di**

[1] Art. 25 del GDPR: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati […]. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".
Lo "stato dell'arte" ivi indicato impone un obbligo, in capo al Titolare (e/o al Responsabile) del trattamento di tenere conto degli attuali progressi tecnologici (disponibili sul mercato), al fine così di determinare le misure di sicurezza (tecniche ed organizzative) adeguate: orbene, esso rappresenta un concetto per natura dinamico, e soggetto ad una continua valutazione (risk assessment); infatti, dinnanzi agli incessanti progressi tecnologici, un Titolare (e/o un Responsabile) del trattamento è tenuto a verificare che una misura che, in passato, era idonea a fornire un adeguato livello di protezione non sia più, invero, attualmente idonea a raggiungere tale obbiettivo, pena la mancata applicazione (e conformità) dell'art. 25 medesimo. In merito, giova aggiungere che il Titolare (e/o il Responsabile) del trattamento è, tuttavia, tenuto a prendere in considerazione i costi di attuazione (da intendersi le risorse in generale, ivi incluso il tempo ed il personale coinvolto) nella scelta e nell'applicazione delle misure di sicurezza tecniche ed organizzative.

[2] Considerando n. 78) del GDPR: "La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e di migliorare caratteristiche di sicurezza. 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 produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a 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, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati…".

[3] L'esame (precoce) di tali principi risulta, peraltro, nell'interesse del Titolare (e/o del Responsabile) del trattamento, in quanto l'assenza del relativo controllo potrebbe rendere gravoso, difficile e costoso apportare modifiche e/o revisioni ad un progetto ovvero lavorazione già in essere.

conseguenza, rispettarli) in modo continuativo, onde così verificare l'efficacia e l'adeguatezza del trattamento, ivi incluse le misure di sicurezza (tecniche ed organizzative) implementate ad esso.
1.2. In altri termini, l'art. 25 del GDPR obbliga ad attribuire rilevanza alle norme comunitarie e nazionali sulla protezione dei dati personali in tutte le fasi del trattamento, compresa quella di ideazione di nuovi processi, prodotti ovvero servizi.

2. Principio di "privacy by design" e di "privacy by default": misure di sicurezza organizzative.
2.1. Il rispetto dei principi in discussione implica l'implementazione non solo di misure di sicurezza tecniche volte a proteggere il trattamento dei dati personali dai rischi derivanti dall'utilizzo di infrastrutture informatiche (o similari), bensì riguarda anche l'adozione di **misure di sicurezza organizzative (adeguate) che possano regolamentare i processi ed i flussi di informazioni e di dati personali all'interno di un'impresa**[4]**, da parametrare in base alla natura** (da qualificarsi con riguardo alla categoria dei dati personali), **alla finalità e**, non da ultimo, **al contesto** (da intendersi in una duplice accezione: tipologia di settore a cui appartiene il Titolare (e/o il Responsabile) del trattamento; circostanze del trattamento, potenzialmente idonee ad influire sulle aspettative del soggetto interessato) **ove vengono svolte le operazioni di trattamento**.
Dunque, risulta necessario predisporre, all'interno di una realtà imprenditoriale, **policy e procedure che siano in linea con i principi sanciti all'interno del GDPR**, e che abbiano lo scopo di prevenire eventi di sicurezza e violazione dei dati personali, minimizzando i dati raccolti, **responsabilizzando e sensibilizzando il personale**, attribuendo ruoli che possano agevolare la verifica del rispetto delle norme, svolgendo DPIA, facilitando gli interessati nell'esercizio dei propri diritti, e predisponendo, ove necessario, procedure di cooperazione con l'Autorità di Controllo (Garante Privacy italiano) idonee ad indirizzare l'impresa verso un efficace (e pronto) riscontro alle richieste derivanti dai poteri ispettivi del competente Garante Privacy.
2.2. Per quanto riguarda la prevenzione degli eventi di sicurezza che possano condurre a violazioni di dati personali, un'impresa è tenuta a formalizzare policy e procedure al fine di rispettare gli artt. 33 e 34 del GDPR.
La presenza di un documento (interno) che descriva come essa prenda in considerazione l'eventualità dell'occorrenza di incidenti di sicurezza che possano compromettere i dati personali da essa trattati, veicolando i flussi informativi interni ed esterni tramite la formalizzazione di procedure che rispettino i dettami degli artt. 33 e 34 del GDPR, implica l'integrazione, sin dalla progettazione, dei processi dell'organizzazione di una sequenza di passaggi che rendono la stessa in grado di diminuire l'impatto di una violazione, di gestirne le fasi per limitare i danni sugli interessati, di regolare efficacemente le comunicazioni e la cooperazione con il competente Garante Privacy, nel rispetto, peraltro, del principio di accountability ex artt. 5 paragrafo 2) e 24 del GDPR[5].
2.3. In aggiunta, si rileva che, all'interno del GDPR (rispettivamente al Considerando n. 39[6] e 83[7]), sono previsti dei principi che, al fine di essere rispettati, implicano l'implementazione di misure organizzative adeguate a prevenire accessi non autorizzati ovvero a

[4] L'EDPB ha precisato, all'interno delle proprie Linee Guida n. 4/2019, che l'art. 25 del GDPR non richiede soltanto l'attuazione di misure tecniche organizzative specifiche, bensì pretende che esse siano idonee (o meglio, efficaci) per l'attuazione dei principi di cui al GDPR in riferimento al trattamento preso in considerazione: così operando, le misure individuate dovrebbero essere idonee ad attuare qualsivoglia ulteriore upgrade finalizzato all'adeguamento rispetto ad un eventuale aumento del rischio (nell'attività di trattamento di specie).
[5] Cfr. Parere n. 3/2010 a firma del WP 29, ove viene affermato – in modo, peraltro, innovativo, rispetto alla relativa formalizzazione all'interno del GDPR – che ciascun Titolare (e/o Responsabile) del trattamento deve mettere in atto misure adeguate, efficaci e concrete per garantire che i principi (e gli obblighi), stabiliti dalla legislazione vigente in materia, siano rispettati, e per dimostrare tale osservanza, su richiesta, alla competente Autorità di Controllo (la quale, pertanto, svolge, per lo più, un'attività ex post e non ex ante, come accadeva sotto la vigenza della precedente (e ora abrogata) Direttiva cd. Madre): dunque, il principio di accountability non va ad influire, in alcun modo, sui principi (fondanti) il GDPR, bensì persegue l'obiettivo di farli funzionare al meglio.
Il medesimo WP 29 ha, peraltro, ricordato che il principio in questione non rappresenta, invero, una novità in sé, dato che il suo (espresso) riconoscimento è ravvisabile nelle Linee Guida per la protezione della vita privata dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) adottate nel 1980, negli standard internazionali di Madrid elaborati dalla Conferenza Internazionale sulla Protezione dei dati e la privacy e, infine, all'interno della Legge canadese "Personal Information Protection and Electronic Documents Act".
[6] Considerando n. 39) del GDPR: "…I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate nel trattamento".
[7] Considerando n. 83) del GDPR: "Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbero valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati personali è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale".

mantenere la riservatezza dei dati personali conservati (e custoditi) all'interno di un'impresa[8]: pertanto, un'ulteriore misura organizzativa riguarda la creazione di un sistema di **lettere d'incarico (atti di nomina) relative al trattamento dei dati personali ed autorizzazioni all'accesso ai sistemi che contengono tali informazioni**; la formalizzazione di policy e procedure in tal senso implica la capacità di sensibilizzare, in modo adeguato, il proprio sistema di gestione delle credenziali di accesso ai vari sistemi ed apparati (ivi inclusi, quelli fisici), al fine così di prevenire il rischio di intrusioni (esterne o interne) che possano compromettere i dati personali oggetto di trattamento.

2.4. Un ulteriore strumento[9] di notevole rilevanza è la **Valutazione d'Impatto** (DPIA) ex art. 35 del GDPR (da eseguirsi, in particolar modo, laddove il trattamento in esame può determinare un rischio (elevato) per i diritti e le libertà del soggetto interessato: es. applicazioni mobili; profilazione; videosorveglianza; geolocalizzazione; dati personali riferiti a soggetti vulnerabili; dati biometrici; dati genetici), la quale è uno degli strumenti principali per parametrare, in modo adeguato, lo sviluppo di nuovi processi, prodotti o servizi in funzione dei principi[10] e delle norme del GDPR: essa è, infatti, funzionale all'individuazione di adeguate misure di sicurezza (tecniche ed organizzative) finalizzate a mitigare i rischi per gli interessati identificati nell'ideazione di processi, prodotti e servizi.

2.5. Il rispetto dei principi in questione è desumibile anche dal rapporto che il Titolare (e/o il Responsabile) del trattamento possiede con i relativi **soggetti interessati**, ai quali deve essere consentito di esercitare, in modo facile ed agevole, i propri diritti, anche grazie all'implementazione di un'apposita procedura organizzativa (interna) tesa a guidare il personale dell'impresa a riscontrare, in modo tempestivo, le richieste degli interessati.

2.6. In ultimo, si sottolinea come la **formazione** delle persone autorizzate a trattare i dati personali sia, invero, tra le più efficaci misure di sicurezza organizzative, giacché idonee ad assicurare che chi entra in contatto con i dati personali sia consapevole dei rischi sottesi al trattamento, dei diritti esercitabili, delle norme e dei principi di cui al GDPR, e delle linee guida redatte, a tal proposito, dall'impresa ove presta la propria attività lavorativa.

2.7. In conclusione, si ricorda che il Titolare (e/o il Responsabile) del trattamento deve essere in grado di **implementare impostazioni** (e, ove necessario, opzioni) **di elaborazione idonee ad elaborare, in modo predefinito, soltanto quei dati personali che sono strettamente necessari per raggiungere lo scopo (legittimo) perseguito**[11]: dunque, il Titolare (e/o il Responsabile) del trattamento è tenuto a non raccogliere dati personali ulteriori (rispetto a quelli, appunto, necessari al trattamento in esame), è tenuto a non conservarli per un periodo di tempo più lungo del necessario[12] e, infine, è tenuto a trattare le informazioni medesime soltanto per quelle finalità espressamente indicate all'interno della specifica informativa ex art. 13 o 14 del GDPR rilasciata, nei termini di legge, ai relativi soggetti interessati[13].

3. Principio di "privacy by design" e di "privacy by default": misure di sicurezza tecniche.

3.1. In primis, è necessario tenere a mente che, stante il fatto che la letteratura relativa alla protezione dei dati personali in fase di progettazione di prodotti, beni ovvero servizi è particolarmente vasta, l'ENISA e l'Information & Privacy Commissioner dell'Ontario (IPCO) risultano, ad oggi, essere le due fonti normative (di secondo livello) che, a parere della dottrina nazionale dominante, sono riuscite ad elaborare dei principi generali in relazione al tema de quo[14].

---

[8] La definizione di chiari profili autorizzativi, la presenza di lettere d'incarico e linee guida al trattamento dei dati personali assume rilevanza in quanto, se correttamente e capillarmente diffuse all'interno di un contesto organizzativo, limitano ex ante la possibilità che si operi al di fuori dei principi stabiliti dal GDPR.

[9] Un'aggiuntiva misura organizzativa consiste nella nomina di un Data Protection Officer nell'ipotesi (tassative) previste dall'art. 37 del GDPR ovvero, come la dottrina raccomanda, laddove sussistono le fattispecie di applicabilità dell'art. 35 del GDPR, ossia nel caso di un trattamento idoneo a determinare un rischio elevato per i diritti (fondamentali) e le libertà degli interessati: infatti, tra i compiti di un DPO vi è quello di controllare e di verificare l'applicazione dei principi e delle norme (comunitarie e nazionali) sulla protezione dei dati personali. Laddove un Titolare (e/o un Responsabile) del trattamento abbia nominato un DPO, l'EDPB incoraggia il coinvolgimento (attivo) di tale figura professionale onde così integrare i principi in questione in ogni fase (e ciclo) del trattamento.

[10] I principi sono delineati nell'art. 5 e Considerando n. 39) del GDPR.

[11] Tale aspetto deve riguardare il volume, la categoria ed il livello di dettaglio dei dati personali richiesti per le finalità di trattamento esplicitate.
Inoltre, un Titolare (e/o un Responsabile) del trattamento deve, innanzitutto, verificare se ha bisogno di trattare i dati personali per il perseguimento delle proprie finalità di trattamento; dopo di che, deve verificare se tali scopi possono essere raggiunti elaborando meno dati personali ovvero disponendo di dati personali meno dettagliati ovvero aggregati.

[12] La finalità del trattamento è il criterio principale per decidere per quanto tempo devono essere conservati i dati personali.

[13] Come precisato dall'EDPB all'interno delle proprie Linee Guida n. 4/2019, il design del trattamento (e, di conseguenza, di raccolta dei dati personali ad esso funzionali) deve, dunque, essere plasmato in ragione di quanto è necessario per il raggiungimento degli scopi del trattamento.

[14] Nel dettaglio, preme precisare che i principi elaborati dall'ENISA sono otto (minimizzare; nascondere; separare; aggregare; informare; controllare; forzare; dimostrare), mentre quelli predisposti dall'ICO sono invece sette (prevenire, non rimediare; privacy by default; privacy insita nel sistema; piena funzionalità; privacy end to end; visibilità e trasparenza; rispetto per l'utente e la sua privacy).

3.2. Fatta questa doverosa (ed importante) premessa, si ricorda che, al fine di raggiungere l'obiettivo di implementare i principi di "privacy by design" e di "privacy by default" è necessario sviluppare tecnicamente applicazioni, prodotti e servizi contenenti misure di sicurezza allo "stato dell'arte".
A tal fine, può essere, senz'altro, utile attuare (o comunque a mente) le seguenti prescrizioni:

- Le applicazioni, i prodotti e/o i servizi (informatici) devono prevedere il superamento di una procedura di autenticazione "robusta"[15], prima di poter permettere il trattamento di qualsiasi dati personale;
- La password scelta (ed utilizzata) dall'utente può essere conservata all'interno dell'applicazione, prodotto e/o servizio, e, in tal caso, deve essere protetta con adeguati algoritmi, in forma criptata; altresì, essa non dovrebbe consentire all'utente il riferimento diretto allo stesso, dovrebbe avere una lunghezza massima di 64 caratteri (e, in via generale, minima di 8 caratteri; dovrebbe contenere lettere minuscole e maiuscole, numeri e caratteri speciali; dovrebbe essere modificata al primo accesso (se non generata dall'utente medesimo), e dovrebbe scadere a sessioni temporali periodiche; in aggiunta, il sistema dovrebbe poter salvare gli hash delle password utilizzate dall'utente, onde così non consentire allo stesso di riutilizzarle;
- In relazione alle cd. web application (ossia, le applicazioni e/o servizi che richiedono la generazione di un token al fine di mantenere attiva la connessione con essi), essa è tenuta a generare un token sufficientemente lungo e non prevedibile che si associ alla sessione, e che sia dotato di un tempo di scadenza che si inneschi come conseguenza dell'inattività dell'utente;
- Nel caso in cui le credenziali di accesso derivino dal processo di un indirizzo e-mail è, d'uopo, necessario verificarne l'esistenza e l'effettiva appartenenza all'utente (e, ove necessario, procedere periodicamente a riverificarne l'attualità del processo);
- Ove necessario, l'applicazione, il prodotto e/o il servizio dovrebbe prevedere la possibilità di attivare un'autenticazione a due fattori, che si basi non solo sul possesso di una password, ma anche sulla generazione di una one time password inviata all'interessato tramite canali alternativi o sul controllo di una componente biometrica o sull'utilizzo di un dispositivo in esclusivo possesso dell'interessato (es. smart card);
- In fase di sviluppo di un'applicazione, prodotto e/o servizio, è opportuno prendere in considerazione la possibilità di limitare o rallentare la procedura di accesso in presenza di tentativi non andati a buon fine, onde così impedire attacchi comuni (es. brute force);
- Ove opportuno, l'applicazione, un prodotto e/o un servizio dovrebbe, inoltre, agevolare la possibilità di gestire le utenze al proprio interno consentendo l'applicazione dei principi di fast privilege e need to know;
- Al fine di garantire la sicurezza del trattamento, l'applicazione, il prodotto e/o un servizio dovrebbe essere predisposto in maniera tale da generare dei log di accesso (dotati delle caratteristiche di completezza, inalterabilità e passibili di verifica di integrità);
- Al fine di riscontrare le richieste di esercizio dei diritti dei soggetti interessati, un'applicazione, prodotto e/o servizio dovrebbe essere sviluppato tenendo in considerazione la possibilità che il dato possa essere soggetto ad accesso, limitazione e cancellazione.

Garbagnate Milanese, lì 9.11.2022 (data di ultimo aggiornamento)

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE
(in persona del suo legale rappresentante pro tempore)

[15] Tale termine è da intendersi come una procedura di autenticazione che deve consistere nella verifica di almeno nome utente e password. Inoltre, applicazioni, prodotti e/o servizi possono essere sviluppati al fine di integrarsi con sistemi di gestione centralizzata degli account, in maniera tale da limitare la produzione di credenziali di autenticazione.