Team RPD/DPO – Indicazioni operative

Il Responsabile Protezione Dati / Data Protection Officer (di seguito, sinteticamente, "RPD/DPO") è una figura introdotta dal Regolamento UE 2016/679 (di seguito "RGPD/GDPR"), la cui individuazione è resa obbligatoria, fra gli altri, per le pubbliche amministrazioni ai sensi dell'art. 37. Al RPD/DPO sono assegnati i compiti previsti in termini generali dall'art. 39 del RGPD/GDPR, che, in osservanza alle "Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea" elaborate in collaborazione con l'Autorità Garante per la protezione dei dati personali nell'ambito del progetto internazionale T4DATA, vengono declinati in termini operativi con il presente documento. Poiché il RGPD/GDPR prevede che al RPD/DPO vengano fornite le risorse necessarie per assolvere i propri compiti, ci si riferirà allo staff costituito dal RPD/DPO stesso e dai propri eventuali collaboratori con la locuzione "Team RPD/DPO".

1. Modalità di contatto

I contatti telefonici diretti con il Team RPD/DPO sono aperti, all'interno 0108497636-7647 (oppure tramite centralino 01084911 per le chiamate dall'esterno dell'Azienda), dal lunedì al venerdì negli orari di servizio.
Oltre tali orari, il RPD/DPO rimane reperibile al numero di cellulare comunicato alla Direzione.
Le strutture che necessitano di incontri (eventualmente anche in video/audio conferenza) per consulenze su problematiche privacy, salve eventuali emergenze, devono richiedere un appuntamento inviando una email all'indirizzo rpd@asl3.liguria.it. Tali incontri devono essere richiesti, preferibilmente, dal dirigente responsabile e/o referente autorizzati con compiti specifici del Sistema Privacy aziendale [1] e/o relativi facilitatori[2], ma analoga possibilità è consentita (ai sensi dell'art. 39, par. 1, lett. a del RGPD/GDPR) al restante personale aziendale, anche per mettere a conoscenza il Team circa la prevista attivazione di nuove attività di trattamento dei dati. Questo consentirà di prevedere, in collaborazione tra il Team RPD/DPO e la/e struttura/e interessate, l'attivazione, sin dall'avvio, dei necessari adempimenti richiesti dalla normativa, nell'ottica dei principi di "protezione dei dati fin dalla progettazione" e "protezione dei dati per impostazione predefinita" previsti dal RGPD/GDPR.
L'indirizzo email del RPD/DPO da comunicare agli utenti dei servizi aziendali, per loro eventuali necessità, come riportato nelle informazioni generali per pazienti e utenti disponibili sul sito istituzionale www.asl3.liguria.it/Politiche della privacy aziendale, è rpd@asl3.liguria.it, oltre ai seguenti indirizzi:

- Via Bertani, 4 16125 Genova (GE)
- **PEC** protocollo@pec.asl3.liguria.it.

2. Nomine privacy per il personale interno

Il RPD/DPO, insieme al proprio eventuale staff, supporta il Titolare del trattamento nella definizione dell' "organigramma privacy" dell'Azienda, in particolare nell'individuazione dei ruoli, ma non delle persone, da nominare quali dirigente responsabile e/o referente autorizzati con compiti specifici del Sistema Privacy aziendale[1]. Ciascun dirigente responsabile e/o referente autorizzati con compiti specifici del Sistema Privacy aziendale [1], avendone la competenza specifica, ha il compito di individuare e designare i propri operatori che trattano dati personali quali "persone autorizzate al trattamento dei dati" o, più brevemente, "autorizzati" secondo le modalità previste in Azienda e salvo che non vi provveda direttamente il Titolare del trattamento.
Il dirigente autorizzato con compiti specifici del Sistema Privacy aziendale [1] responsabile della Struttura aziendale S.I.A. è tenuto ad individuare gli ambiti di attività dei propri amministratori di sistema, così da consentirne un'adeguata designazione, da aggiornare periodicamente. Il Team propone al Titolare del trattamento modalità di monitoraggio sulle designazioni effettuate dalle diverse strutture.

3. Nomine privacy per i soggetti esterni

Le designazioni dei soggetti esterni quali responsabili (ai sensi dell'art. 28 del RGPD/GDPR) vengono predisposte dalle strutture aziendali deputate a gestire i relativi rapporti contrattuali o convenzionali, quindi competenti ai sensi del sistema di gestione della privacy aziendale, e sottoposte al Titolare o suo delegato alla firma per la sottoscrizione. Spetta a queste la predisposizione e l'invio della nomina. In tali operazioni, il Team RPD/DPO può essere di supporto al fine di valutare il ruolo privacy del soggetto esterno, nella

[1] se previsto in Azienda, indicare la denominazione assegnata al ruolo noto, ai sensi della previgente normativa, come "Responsabile interno" (es. Referente Privacy, Soggetto delegato, Soggetto Preposto etc, …)
[2] se individuato all'interno dell'Azienda, indicare la denominazione assegnata al ruolo di supporto (es. Coordinatore Privacy, Referente Privacy etc.)

formulazione dei contenuti del relativo atto di nomina e, qualora emergano le condizioni per una contitolarità, nella definizione dei contenuti dell'accordo di cui all'art. 26 del RGPD/GDPR.
Nel caso in cui le designazioni a Responsabile del trattamento ex art. 28 del RGPD/GDPR prevedano un trasferimento di dati verso Paesi terzi, il Team può supportare il Titolare nella valutazione del rispetto dei requisiti di cui al Capo V del RGPD/GDPR.

4. Registro delle attività di trattamento

Il costante e tempestivo aggiornamento del registro delle attività di trattamento, previsto dall'art. 30 del RGPD/GDPR, è competenza della singola struttura ed in particolare del suo dirigente responsabile autorizzato con compiti specifici del Sistema Privacy aziendale [1]. Il dirigente – referente responsabile della struttura-area autorizzato con compiti specifici del Sistema Privacy aziendale [1] può delegare tale compito al proprio facilitatore[2], mantenendone però la responsabilità. Ove richiesto, il Team RPD/DPO supporta gli operatori, in particolare, nella valutazione di casistiche dubbie, si occupa di svolgere verifiche in ordine ad eventuali anomalie riscontrate nonché di richiedere eventuali modifiche e/o integrazioni.

5. Analisi del rischio e valutazione di impatto

Il RPD/DPO supporta il Titolare nel fornire indicazioni e linee guida per la realizzazione dell'analisi del rischio (relativa ai diritti e alle libertà fondamentali degli interessati), affidata ai dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale[1] nell'ambito della struttura-area di competenza. Il RPD/DPO, insieme al proprio eventuale staff, effettua un monitoraggio della situazione sulla base delle analisi ed informazioni messe a disposizione dal dirigente – referente responsabile della struttura-area autorizzato con compiti specifici del Sistema Privacy aziendale [1] (ed eventualmente dal relativo facilitatore[2]), al fine di evidenziare prioritariamente i trattamenti a rischio elevato per i diritti e le libertà delle persone fisiche e favorire l'adozione delle misure atte al contenimento dello stesso. In tali casi – e comunque in quelli indicati dall'Autorità Garante nell'apposito provvedimento n.467 dell'11 ottobre 2018 –, fornisce indicazioni ai dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1] (e ai relativi facilitatori[2]) per la realizzazione della valutazione di impatto sulla protezione dei dati (DPIA) e, se richiesto, un parere, sorvegliandone lo svolgimento ai sensi degli articoli 35 e 39 par. 1 lett. c) del RGPD/GDPR.

6. Violazioni dei dati personali

In caso di eventuali violazioni di dati personali, sia reali che presunte, il RPD/DPO deve essere contattato secondo la policy aziendale, denominata "Policy aziendale in caso di violazione privacy (data breach)" e nel D.P.S. e consultabile sul sito intranet aziendale Normativa/Privacy/normativa e sul sito istituzionale www.asl3.liguria.it/Politiche della privacy aziendale.

7. Richieste del personale

Qualora un operatore dell'Azienda, sia un dipendente che una figura ad esso assimilabile, rilevi problematiche, reali o presunte, relative al trattamento dei propri dati personali da parte dell'Azienda medesima, può richiedere un appuntamento con il RPD/DPO mediante i contatti riportati al punto 1. Allo stesso modo, gli operatori aziendali possono segnalare al RPD/DPO l'eventuale esistenza o la prossima attivazione di procedure in contrasto, anche solo parziale, con la normativa privacy. È opportuno, però, che la medesima segnalazione venga anche preventivamente rivolta al dirigente – referente responsabile della struttura-area autorizzato con compiti specifici del Sistema Privacy aziendale [1] della struttura di afferenza.
Nelle fattispecie sopracitate non rientrano né la segnalazione di eventuali data breach né l'esercizio dei diritti, che seguono percorsi diversi, come illustrato, rispettivamente, al punto 6 e al punto 8.

8. Esercizio dei diritti degli interessati

Il RPD/DPO, qualora non contattato direttamente all'indirizzo email riportato nelle informazioni generali per pazienti e utenti e richiamato al punto 1, deve essere tempestivamente informato di ogni eventuale richiesta di esercizio dei diritti, di cui agli artt. 15-22 del RGPD/GDPR, o di altre questioni sollevate dagli interessati relativamente al trattamento dei loro dati personali. Il RPD/DPO chiederà la collaborazione delle strutture coinvolte nella richiesta, che saranno tenute a garantirla fino alla predisposizione della risposta e all'invio della stessa all'interessato secondo le modalità previste dalle policy aziendali in materia.

---

[1] se previsto in Azienda, indicare la denominazione assegnata al ruolo noto, ai sensi della previgente normativa, come "Responsabile interno" (es. Referente Privacy, Soggetto delegato, Soggetto Preposto etc, …)
[2] se individuato all'interno dell'Azienda, indicare la denominazione assegnata al ruolo di supporto (es. Coordinatore Privacy, Referente Privacy etc.)

9. Incontri periodici
L'Team RPD/DPO, laddove ritenuto opportuno dal Titolare, convoca incontri con i dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1]o i relativi facilitatori [2] delle strutture-aree. Tali incontri sono mirati a fornire indicazioni operative utili per il rispetto degli adempimenti richiesti dalla normativa, supporto nella soluzione delle problematiche e, qualora presenti, brevi aggiornamenti sull'evoluzione legislativa.

10. Formazione
L'intero personale aziendale, siano essi dipendenti o assimilati, è tenuto a sottoporsi alla formazione periodica in materia di protezione dei dati personali, in quanto tale adempimento costituisce obbligo di legge e misura di sicurezza ai sensi del RGPD/GDPR. Il Team RPD/DPO può proporre sessioni di formazione in aula e/o corsi in modalità FAD al fine di supportare gli operatori nelle attività quotidiane di trattamento dei dati personali. La gestione amministrativa di tali eventi è affidata alla struttura Aggiornamento e Formazione.
In ottemperanza all'art. 37, par. 2 del RGPD/GDPR, l'Azienda è tenuta a fornire al Team RPD/DPO le risorse necessarie a garantire il mantenimento e l'aggiornamento della propria conoscenza specialistica[3].

11. Misure di sicurezza
La struttura SIA definisce ed analizza, a supporto dei dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1] delle strutture-arre utilizzatrici, le misure di sicurezza da applicarsi nei trattamenti informatici di dati personali, contribuendo a valutare la loro adeguatezza "per garantire un livello di sicurezza adeguato al rischio". Il Team RPD/DPO interagisce con tale struttura, fornendo, a seconda delle casistiche in esame, consulenza sulle misure e supporto nella predisposizione e nell'aggiornamento di policy di sicurezza da diffondere alla popolazione aziendale.
Ogni dirigente – referente responsabile della struttura-area autorizzato con compiti specifici del Sistema Privacy aziendale [1] è tenuto ad applicare personalmente ed a garantire il rispetto dell'applicazione delle opportune misure di sicurezza, relative sia ai trattamenti informatici sia a quelli cartacei, nella struttura di competenza.

12. Audit
Il Team effettua audit periodici a campione, all'interno delle strutture aziendali. Ogni audit serve a verificare la messa in atto di misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia svolto in conformità con i principi del Regolamento UE 2016/679, del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e dei Provvedimenti del Garante per la protezione dei dati personali rilevanti in relazione ai trattamenti svolti. Durante gli audit, viene redatto un sintetico verbale che, una volta firmato da tutti i presenti, è trasmesso alla Direzione oltre che alle strutture interessate, così da evidenziare tempestivamente le eventuali non conformità rilevate e/o le azioni di miglioramento suggerite. Ad ogni audit potrà seguire un incontro di approfondimento utile a controllare la correzione delle eventuali anomalie riscontrate. L'ordine, la calendarizzazione e l'organizzazione degli audit viene deciso dal RPD/DPO, a seconda delle priorità e delle criticità emerse.
I dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1] possono comunque richiedere che la loro struttura-area sia sottoposta a tale verifica, sfruttando i contatti riportati al punto 1.

13. Collaborazione con le altre strutture aziendali
Il Team RPD/DPO svolge le proprie funzioni interagendo con le strutture aziendali. Laddove lo ritenga necessario, il Team ha la facoltà di richiedere la collaborazione delle strutture che riterrà di dover necessariamente coinvolgere per la risoluzione delle singole problematiche rilevate o sottoposte alla sua attenzione. Le strutture contattate sono tenute a fornire la collaborazione richiesta.

14. Metodologia di lavoro
Il Team RPD/DPO lavora per priorità. Le richieste di consulenza relative a problematiche di impatto aziendale o interstrutturale hanno la precedenza su quelle riguardanti singole strutture. Tra le richieste interne, la massima priorità è assegnata alla valutazione di eventuali situazioni di data breach.
Qualora le richieste di consulenza si estendano su ambiti trasversali all'Azienda, spetta al responsabile dell'attività procedere al necessario coordinamento delle diverse strutture coinvolte, favorendo, laddove necessario, il confronto tra i diversi professionisti, e procedendo poi alla sintesi conclusiva. Negli ambiti di interesse regionale, per i quali potrebbe essere necessario un confronto con il Gruppo di Lavoro Privacy Regionale, istituito con Deliberazione di A.Li.Sa. n.173 del 06.07.2018, di cui il RPD/DPO, eventualmente coadiuvato dal dirigente responsabile della struttura SIA e dal Team, fa parte, tale compito è in carico al responsabile di progetto.

---

[1] se previsto in Azienda, indicare la denominazione assegnata al ruolo noto, ai sensi della previgente normativa, come "Responsabile interno" (es. Referente Privacy, Soggetto delegato, Soggetto Preposto etc, …)
[2] se individuato all'interno dell'Azienda, indicare la denominazione assegnata al ruolo di supporto (es. Coordinatore Privacy, Referente Privacy etc.)
[3] sul punto, in caso di RPD/DPO esterno, si rinvia ai termini stabiliti dal contratto di servizio

Per consentire al RPD/DPO di svolgere il proprio lavoro e all'Azienda di attuare i principi di "protezione dei dati fin dalla progettazione" e "protezione dei dati per impostazione predefinita", risulta necessario metterlo a conoscenza delle nuove attività tempestivamente e dunque prima che le stesse vengano compiutamente definite e prima che vengano avviate.
In merito alle richieste esterne, fatta salva la precedenza assoluta da assegnare ad eventuali richieste dell'Autorità Garante (che il RPD/DPO ha anche la facoltà di contattare, laddove opportuno, nei limiti di quanto normativamente previsto), le richieste degli interessati ricevono la priorità.

15. Posizione del RPD/DPO

Il parere del RPD/DPO non è vincolante.
Con riferimento alle modalità di scelta del RPD/DPO, si rinvia all'art. 37 del RGPD/GDPR e alle Linee Guida adottate dal Gruppo di Lavoro art. 29 in data 13.12.2016.
Il RPD/DPO non può, in nessun caso, ricevere istruzioni sullo svolgimento del proprio operato e delle proprie funzioni. Tale professionista, insieme al proprio Team, può suggerire metodologie, strumenti e best practice, ma il potere autorizzatorio resta al Titolare e ai dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1] dallo stesso designati per i rispettivi settori aziendali di competenza, che hanno facoltà di scegliere soluzioni diverse. In tale ipotesi, come raccomandato dai Garanti Europei quale buona prassi, è opportuno documentare le motivazioni che hanno portato a condotte difformi da quelle suggerite dal RPD/DPO in modo da poterle esibire in caso di ispezioni.
Né il RPD/DPO né, tantomeno, i componenti del relativo Team possono sostituirsi alla direzione strategica o ai dirigenti delle strutture. Il Team, dunque, non ha competenza:

- ✓ su scelte organizzative;
- ✓ in ambiti specifici e trasversali all'Azienda che, anche per i correlati aspetti giuridici, esulino dalla materia della privacy;
- ✓ sull'approvazione di modulistica o procedure (su di esse, il RPD/DPO può solo esprimere un parere);
- ✓ sulla compilazione dei consensi informati ai trattamenti sanitari quale fattispecie distinta dal consenso al trattamento dati;
- ✓ su questioni quali l'esercizio del diritto di accesso, nelle sue varie declinazioni (documentale, civico o civico generalizzato);
- ✓ nell'ambito di procedimenti amministrativi.

Il RPD/DPO può esclusivamente esprimere un parere finalizzato alla tutela e alla protezione dei dati personali, supportando, in tal senso, il Titolare e collaborando con i dirigenti-referenti responsabili autorizzati con compiti specifici del Sistema privacy aziendale [1] dallo stesso designati per i rispettivi settori aziendali di competenza nonché con le strutture aziendali come detto al precedente punto 13. Il RPD/DPO inoltre ha il compito di assistere il Titolare nel monitoraggio interno della conformità al RGPD/GDPR, operando con continuità, come specificato dal Gruppo di Lavoro art. 29 nelle sue Linee guida sui RPD (approvate dal Comitato Europeo per la protezione dei dati – EDPB), in particolare nella raccolta di informazioni per identificare le attività di trattamento, nell'analisi e nel controllo della loro conformità, nella periodica revisione dei rischi, e nell'informazione, nell'attività di consulenza (anche relativamente, a titolo esemplificativo e non esaustivo, all'eventuale sottoscrizione da parte del Titolare di un codice di condotta e/o al conseguimento di una certificazione ex artt. 40 e 42 del RGPD/GDPR) e di elaborazione di raccomandazioni destinate al Titolare.

[1] se previsto in Azienda, indicare la denominazione assegnata al ruolo noto, ai sensi della previgente normativa, come "Responsabile interno" (es. Referente Privacy, Soggetto delegato, Soggetto Preposto etc, …)