
# Linee guida sul data protection by design e by default

**INFORMAZIONI DOCUMENTO:**

| | | | |
|---|---|---|---|
| **Titolo** | Linee guida sul data protection by design e by default | | |
| **Data di emissione** | 25/05/2018 | **Versione** | 1.0 |

## SOMMARIO

# I. INTRODUZIONE

## A. SCOPO

Le presenti "Linee guida sul data protection by design e by default" hanno lo scopo di illustrare come l'Azienda Ospedale San Raffaele S.r.l. (**"Azienda"**) abbia adottato presidi interni (es. policy/procedure, misure di sicurezza) volti a far sì che i Trattamenti di Dati Personali svolti dalla medesima siano allineati a questi nuovi principi.

Salvo diversamente previsto all'interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni presenti nel GDPR e riportate per comodità nella sezione "Glossario e Acronimi".

## B. NORMATIVA DI RIFERIMENTO

Articolo 25

**Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del 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, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. 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.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

## C. DOCUMENTI DI RIFERIMENTO

1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
2. Procedura per la gestione dei Data Breach
3. Procedura sulla cooperazione con l'Autorità di Controllo
4. Linee guida sulle Persone Autorizzate al Trattamento dei Dati Personali
5. Linee guida per il Responsabile del Trattamento dei Dati Personali
6. Procedura sull'esercizio dei diritti dell'Interessato
7. Procedura sul Data Protection Impact Assessment

8. Privacy Policies
9. Questionario Trattamenti dipendenti
10. Linee guida sulla base giuridica del Trattamento
11. Procedura sull'Analisi dei Rischi IT
12. "Linee guida in materia di Dossier sanitario" del 4 giugno 2015 – G.U. n. 164 del 17 luglio 2015
13. "Prescrizioni in tema di Fascicolo sanitario elettronico (Fse)" del 16 luglio 2009 - G.U. n. 178 del 3 agosto 2009.
14. Linee guida in tema di referti on-line 19 novembre 2009
15. Provvedimento in materia di videosorveglianza 8 aprile 2010
16. Linee guida per il trattamento di dati personali nell'ambito delle sperimentazioni di medicinali 24 luglio 2008
17. Linee guida sul trattamento di dati personali dei lavoratori privati 23 novembre 2006
18. 
19. linee guida in tema di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario 5 maggio 2011
20. DPCM n.178/2015 «Regolamento in materia di FSE» e DM 4 agosto 2017 Interoperabilità che prevedono l'adozione di una nuova versione dell'informativa sul trattamento dei dati personali.

## D. GLOSSARIO E ACRONIMI

**Archivio:** qualsiasi insieme strutturato di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

**Aree Sensibili:** sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;

**Autorità di Controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;

**Consenso dell'Interessato** o **Consenso**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

**Dati Biometrici:** i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

**Dati Comuni:** sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;

**Dati Genetici:** i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

**Dati Giudiziari:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

**Dati Particolari:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

**Dati relativi alla Salute:** i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

**Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“**Interessato**”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

**Destinatario/i**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

**Device Fissi**: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

**Device Mobili**: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

**DPO** o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all’art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

**GDPR** o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

**Gruppo Imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

**Incaricato/i o Persona/e Autorizzata/e:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dell'Azienda e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

**Limitazione Di Trattamento:** il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

**Processo Decisionale Automatizzato:** decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

**Profilazione:** qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

**Pseudonimizzazione:** il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

**Rappresentante:** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

**Responsabile del Trattamento** o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare

garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

**Rete Aziendale:** rappresenta il perimetro digitale dell'Azienda, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN);

**Strumenti Aziendali**: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dall'Azienda alle Persone Autorizzate al fine di svolgere le proprie mansioni;

**Strumenti Personali**: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

**Terzo:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;

**Titolare del Trattamento** o **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

**Trattamento** o **Trattato/Trattati:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

**Trattamento Transfrontaliero:** a) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del Trattamento o Responsabile del Trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

**Violazione Dei Dati Personali** ovvero **Data Breach:** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

**Dossier sanitario Elettronico:** l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica a vantaggio dei professionisti sanitari che presso lo stesso titolare del trattamento lo assistono. Rappresenta un trattamento di dati personali specifico, volto a documentare parte della storia clinica dell'interessato attraverso la realizzazione di un sistema integrato delle informazioni sul suo stato di salute accessibile da parte del personale sanitario che lo ha in cura.

Fascicolo sanitario elettronico: l'insieme dei dati personali originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es. azienda sanitaria, laboratori clinici privati operanti nella medesima Regione).

## II. IL PRINCIPIO DI DATA PROTECTION BY DESIGN

La Direttiva 95/46/CE rinviava indirettamente alla tutela dei Dati Personali sin dalla progettazione (cd. "*data protection by design*"), ad es. con l'art. 17 relativo alle «*misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali*». Lo stesso rinvio è operato dalla Direttiva 2000/58/CE che all'art. 14.3 precisa: «*All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali* [...]». Tuttavia, nonostante le predette disposizioni delle due direttive siano state utili ai fini della promozione della protezione dei dati e della vita privata fin dalla progettazione, esse non hanno mai avuto un'effettiva applicazione sufficiente ad assicurare l'integrazione della *data protection* e della privacy "*by design*".

All'interno del Regolamento invece, per invitare al rispetto del principio di *data protection-by-design* l'art. 25 parla esplicitamente di "Protezione dei dati fin dalla progettazione". La predetta disposizione, letta in combinato con il Considerando 78 dello stesso GDPR, prevede che i produttori dei prodotti, dei servizi e delle applicazioni basati sul Trattamento di Dati Personali o che Trattano Dati Personali per svolgere le loro funzioni, in fase di sviluppo, progettazione, selezione e utilizzo di tali strumenti, dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati in modo da adempiere ai loro obblighi di protezione dei dati.
È evidente, dunque, come il Considerando 78 del RGPD combini lo sviluppo e la progettazione di prodotti e servizi da parte dei produttori con il principio di *accountability* del Titolare o del Responsabile che utilizzeranno quelle tecnologie, rendendo così la *data protection-by-design* un criterio di valutazione della responsabilità stessa di questi soggetti.
Si noti che il valore dell'introduzione del principio di *data protection-by-design* (e della protezione dei dati come opzione predefinita – cd. *data protection-by-default*), di cui all'art. 25, è esplicitato non solo nell'inclusione del predetto articolo tra le circostanze che possono essere valutate dall'Autorità di Controllo competente al momento di comminare una sanzione amministrativa, ma soprattutto nell'inclusione della mancata applicazione dei principi di cui all'art. 25 tra le condotte passibili di sanzione da parte della Autorità di Controllo, *ex* art. 83.4.a) – cioè fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato globale se superiore.

## III. L'APPLICAZIONE DEL PRINCIPIO DI DATA PROTECTION BY DESIGN

Tenuto conto dell'obbligatorietà del rispetto del principio di *data protection-by-design* che emerge dalle disposizioni del GDPR, si illustrano di seguito delle brevi linee guida relative all'applicazione della *data protection-by-design* in processi e prodotti o servizi dell'Azienda.

Integrare la *data protection-by-design* nelle procedure intraprese significa proteggere i Dati personali attraverso misure sia tecniche che organizzative, adottate *ex ante* rispetto al verificarsi dell'evento dannoso.

In tal senso, **gli ambiti che necessitano di includere, sin dalla loro progettazione, la protezione dei dati sono sostanzialmente tre:**

- **obblighi e adempimenti in materia di sicurezza;**
- **obblighi e adempimenti di garanzia nei confronti dei diritti dell'Interessato;**
- **collaborazione con soggetti preposti al controllo**.

### A. MISURE DI SICUREZZA

Dal punto di vista tecnico, è necessario integrare le misure di sicurezza direttamente in applicazioni, servizi e prodotti, sin dalla fase di loro sviluppo e progettazione. Seguendo le disposizioni dell'art. 32 GDPR, infatti, prodotti, servizi e applicazioni dovrebbero prevedere *ex ante* misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che possono comprendere la Pseudonimizzazione e la cifratura dei Dati Personali, nonché assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento attraverso procedure tecniche che consentano di «*ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*» (*ex* art. 32 GDPR).

Beninteso, integrare la *data protection-by-design* nelle misure di sicurezza non significa dare per assodate e immutabili le misure inserite in fase di progettazione. È infatti necessario, ai sensi dell'art. 32.d) GDPR stabilire una procedura interna volta a «*testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*». Sul punto, l'Azienda predispone al proprio interno audit periodici, tecnologici, documentali e organizzativi, nonché svolge regolarmente, per esempio, prove di penetrazione nel perimetro informatico aziendale sulle misure di sicurezza adottate nei diversi sistemi di Trattamento con strumenti informatici. La stessa premura è imposta ai Responsabili del Trattamento attraverso una Checklist Privacy e il Contratto per il Trattamento dei Dati Personali contenuti nelle Linee Guida per il Responsabile del Trattamento dei Dati Personali.

Nel valutare l'adeguato livello di sicurezza, infine, l'Azienda, per integrare il principio di *data protection-by-design* nelle misure di sicurezza, "*tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*" (cfr. art. 32 (2) GDPR) attraverso una Procedura sull'Analisi dei Rischi IT.

## B. PROCEDURA PER LA GESTIONE DEI DATA BREACH

Con riferimento agli obblighi in materia di sicurezza, è necessario prevedere sin dalla progettazione di applicazioni, prodotti e servizi, delle contromisure organizzative effettive e tempestive al fine di procedere alla notificazione all'Autorità di Contratto competente (*ex* art. 33 GDPR) e alla comunicazione all'Interessato (*ex* art. 34 GDPR) in caso di Violazione dei Dati Personali (cfr. Procedura per la gestione dei Data Breach). A ben vedere, in effetti, il ripristino della sicurezza *ex post* rispetto al verificarsi della violazione, passa per l'integrazione sin dalla progettazione sia di misure di sicurezza adeguate, sia di sistemi di risposta efficienti che a seguito della violazione consentano di adempiere agli obblighi di collaborazione con l'Autorità di Controllo (cfr. Procedura sulla cooperazione con l'Autorità di Controllo) e di garantire all'Interessato il rispetto dei suoi diritti (cfr. Procedura sull'esercizio dei diritti dell'Interessato).

## C. SISTEMA DELLE AUTORIZZAZIONI E NOMINE

È bene precisare che tra le misure intraprese *ex ante*, introdotte sin dalla progettazione di prodotti e servizi, non rientrano solo quelle tecniche (ad es. Pseudonimizzazione) o organizzative (ad es. Procedura per la gestione dei Data Breach) messe in atto per gestire le informazioni, la loro salvaguardia e difesa in caso di intrusioni e alterazioni non autorizzate. Infatti, vi sono anche tutte quelle misure organizzative che riguardano il sistema delle autorizzazioni relative all'accesso ai dati (cfr. Linee guida sulle Persone Autorizzate al Trattamento di Dati Personali); i Contratti per il Trattamento di Dati Personali (cfr. Linee Guida per il Responsabile del Trattamento dei Dati Personali) - l'esecuzione della valutazione di impatto sulla protezione dei dati (cfr. Procedura sul Data Protection Impact Assessment) e tutte quelle ulteriori misure organizzative funzionali a custodire e controllare i dati.

Procedendo con ordine, il sistema delle nomine appare necessario nel rispetto del principio di riservatezza intesa nel senso introdotto dal Considerando 83, il quale menziona esplicitamente la riservatezza come adeguato strumento di sicurezza dei dati, proprio perché l'obiettivo del Titolare deve essere quello di impedire anche l'accesso o l'utilizzo non autorizzato dei Dati Personali e delle attrezzature impiegate per il Trattamento (cfr. Considerando 39). Alla luce di questa considerazione, la presenza di mansionari e lettere di incarico a Persona Autorizzata al Trattamento (già "incaricati") diventano necessarie in quanto definiscono i profili di autorizzazione e impongono ai Responsabili del Trattamento di attenersi alle istruzioni impartite dal Titolare evitando *by design* che vi sia accesso ai, o utilizzo non autorizzato dei, Dati Personali. Le designazioni, in sostanza, consentono di distribuire sin da subito, prima che avvenga il Trattamento, le responsabilità tra Titolare e Responsabile, attribuendo a quest'ultimo una serie di obblighi, affinché non solo egli operi soltanto su istruzioni del Titolare (cfr. Linee Guida per il Responsabile del Trattamento dei Dati Personali) — ma anche applichi una serie di misure tecniche e organizzative volte al Trattamento lecito dei dati, coadiuvando così il Titolare nell'esecuzione degli obblighi a lui attribuiti.

## D. NOMINA DEL DATA PROTECTION OFFICER

Parimenti, la nomina di un responsabile per la protezione dei dati (DPO) costituisce una misura organizzativa che consente di rispettare il principio di *data protection-by-design*, in quanto tale figura svolge diversi compiti tra cui la sorveglianza sull'applicazione del GDPR da parte dell'Azienda e sul rispetto «*delle politiche del titolare del trattamento o del responsabile*». La sua funzione è proprio quella di garantire l'implementazione della protezione dei dati *ab origine*, assicurando agli Interessati una tutela che va oltre la semplice applicazione della norma, grazie alla maggiore consapevolizzazione del Titolare e del Responsabile rispetto ai rischi del Trattamento e agli strumenti per mitigarli (cfr. Determinazione sulla designazione e compiti del DPO).

## E. POLICY

Le politiche (policy, procedure, linee guida interne, circolari), a loro volta, vanno annoverate tra le misure organizzative che implementano la protezione dei dati sin dalla progettazione di prodotti, servizi o applicazioni, in quanto consentono di modellare il Trattamento dei Dati Personali su regole dettate in principio (cfr. sezione Utilizzo della Rete Aziendale in Policy sugli strumenti IT).

## F. FORMAZIONE

Da non sottovalutare è, poi, la formazione di ogni Persona Autorizzata a Trattare i Dati Personali, che ricade tra le misure di natura organizzativa, grazie alla quale è possibile assicurarsi che chi materialmente tratta i Dati Personali per conto dell'Azienda conosca regole e potenziali rischi di tale attività (cfr. Linee guida sulla formazione e – *de relato* - Linee guida sulle Persone Autorizzate al Trattamento di Dati Personali)

## G. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI ("DPIA")

Il DPIA o Valutazione d'impatto sulla protezione dei Dati Personali è il cuore applicativo del principio di *data protection-by-design*, è disciplinato dall'art. 35 del GDPR e ha l'obiettivo non solo di garantire la sicurezza dei Dati Personali, ma soprattutto di individuare i rischi specifici del Trattamento. Il legame tra DPIA e *data protection-by-design* risiede proprio nel fatto che esso è prodromico rispetto all'adozione delle adeguate misure di sicurezza che vanno implementate nei prodotti e servizi che Trattano Dati Personali. Il concetto di sicurezza, dunque, riguarda la protezione dei dati sin dalla progettazione di applicazioni, prodotti e servizi in quanto essa dipende proprio dal rapporto tra Trattamento e diverse tipologie di dati Trattati. Inoltre, il DPIA consente all'Azienda di affrontare gli aspetti di protezione dei dati prima che il prodotto o il servizio vengano messi sul mercato. Ciò fa sì che si riduca l'incertezza giuridica rispetto ai rischi, generando vantaggi sia per gli Interessati sia per le filiere di soggetti attivi del Trattamento di dati (Titolari, Responsabili, Sub-Responsabili).

Fatto salvo l'uso della Procedura sul Data Protection Impact Assessment per le progettualità nuove e quelle esistenti, esempio pratico di DPIA come strumento per implementare il principio di *data protection-by-design* è quello adottato dall'Azienda con riferimento ai Trattamenti dei Dati Personali dei propri dipendenti e collaboratori.

Ogni qualvolta venga proposta una nuova tecnologia, applicativo o servizio addizionale ad uno preesistente (es. *fingerprint*, videosorveglianza, applicativi aziendali per *remote working* ecc), l'Azienda fa compilare e tiene aggiornato un questionario che elenca i Trattamenti che secondo Il Gruppo di Lavoro Articolo 29[1] comportano alti rischi per privacy dei dipendenti e collaboratori (cfr. Questionario Trattamenti dipendenti riportato in calce per riferimento, ma presente in formato Office Excel per una più facile compilazione). Se la progettualità rientra tra gli esempi elencati, l'Azienda procede ad analizzarla sotto la lente di ingrandimento della Procedura sul Data Protection Impact Assessment.

## H. DIRITTI DEGLI INTERESSATI, OBBLIGHI INFORMATIVI, BASI DI LICEITÀ

Con riferimento al profilo della garanzia dei diritti dell'Interessato e i relativi obblighi e adempimenti, si noti che, se da un lato i Dati Personali divengono sempre più preziosi per il Titolare, dall'altro anche gli Interessati sono più consapevoli della loro rilevanza. Ciò implica la necessità di applicare *by design* misure tecniche, ma soprattutto organizzative, che non solo riducano al minimo i rischi, ma che consentano di sviluppare un rapporto di fiducia con gli Interessati e di mantenere una buona relazione con essi.
In tal senso, l'Azienda fornisce a ciascun Interessato l'informativa privacy prevista dagli artt. 13 e 14 GDPR (cfr. Privacy Policies) in cui sono indicate le condizioni di liceità del Trattamento (es. consenso, legittimo interesse ex artt. 6 e 9 GDPR) preventivamente valutate dall'Azienda nelle Linee guida sulla base giuridica del Trattamento. Non solo: deve essere anche progettato un sistema di CRM che implichi la stratificazione del database, in modo tale da poter registrare e conservare le informative, le domande di Consenso (o la base legale prescelta) e le risposte date da ciascun Interessato, tenendo traccia nel tempo anche degli eventuali cambiamenti di volontà dell'Interessato con riferimento ad uno o più trattamenti di Dati Personali.

Altrettanto fondamentale è la definizione *ex ante* di una idonea organizzazione per fornire riscontro tempestivo alle istanze dell'interessato (art. 12.3 GDPR) nonché per permettere al medesimo l'esercizio dei diritti a lui riconosciuti dagli artt. 15-22 GDPR. A tal proposito, l'Azienda si è dotata di una Procedura sull'esercizio dei diritti dell'Interessato.

## I. COLLABORAZIONE TRA SOGGETTI DI CONTROLLO

In ultimo, con riferimento alla collaborazione con i soggetti preposti al controllo, per la quale l'Azienda ha adottato una Procedura sulla cooperazione con l'Autorità di Controllo, la *data protection-by-design* può essere individuata come essenziale nella progettazione di tutte quelle procedure che consentono la conservazione delle prove relative alla *compliance* con le disposizioni del GDPR: il Registro dei Trattamenti ex art. 30, gli esiti del DPIA, gli archivi di nomine, incarichi, contratti ecc.

[1] ec.europa.eu/newsroom/document.cfm?doc_id=45631

# J. APPENDICE

## 1) LINEE GUIDA DI DATA PROTECTION BY DESIGN PER IL DOSSIER SANITARIO ELETTRONICO

a) Il sistema deve essere predisposto per la possibile cancellazione automatica, dopo un periodo di tempo prestabilito, dei dati personali e/o per la loro anonimizzazione in forma irreversibile e dare evidenza della avvenuta cancellazione del dato; ad esempio ciò è reso possibile attraverso la implementazione di un cronjob (a livello generale o applicazione per applicazione) che controlla la presenza di eventuali dati in scadenza e procede alla loro cancellazione tempestiva. Tale cronjob potrebbe documentare l'operazione di cancellazione su un log inalterabile, completo e di cui può essere verificata l'integrità. I dati possono essere alternativamente anonimizzati (e non pseudonimizzati).

b) Il sistema deve rendere possibile l'export del/i dato/i in formato elettronico interoperabile aperto di uso comune (es. CSV, XML, JSON, ecc.…).

c) Il sistema deve essere in grado di "congelare"[2] uno o più dati personali dell'interessato che ha esercitato il diritto di opposizione e/o limitazione e "contrassegnare" temporaneamente il/i dato/i personale/i "congelato/i".

d) Il sistema deve disporre di un pannello consultabile dagli operatori sanitari, nel quale sono annotati gli estremi dell'acquisizione dei consensi o di altre opzioni privacy espresse dall'interessato (es. l'oscuramento dei dati personali); una volta annotati i consensi e le altre opzioni privacy, il sistema deve essere in grado di modificare automaticamente i flussi di dati e i profili di autorizzazione per l'accesso ai dati.

e) Il sistema deve consentire l'oscuramento di un dato clinico/sanitario in modo tale da garantire che i soggetti abilitati all'accesso, ma esclusi dalla visualizzazione, non possano venire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").

f) Il sistema deve consentire un'organizzazione dei dati modulare al fine di un accesso selettivo ai dati personali in esso contenuti, da parte dei diversi soggetti abilitati.

g) Il dispositivo deve essere dotato di un sistema che registra e conserva per almeno 24 mesi i log di accesso o il tentativo di accesso ai dati e le operazioni compiute (anche di mera inquiry) tenendo traccia almeno delle seguenti informazioni:
   - data e ora di esecuzione;
   - codice della postazione di lavoro utilizzata da chi ha effettuato l'accesso;
   - identificativo del paziente/soggetto a cui i dati si riferiscono;

[2] impedire il temporaneo trattamento del dato/i, a parte la mera conservazione.

- tipologia dell'operazione compiuta sui dati.

h) Il sistema deve prevedere l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento che vi accedono (ad es., relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

i) Il sistema deve prevedere una apposita sezione consultabile dall'interessato da cui può verificare gli accessi eseguiti sul proprio dossier sanitario in qualunque momento (data e ora di esecuzione, tipologia dell'operazione compiuta sui dati; reparto/unità operativa da cui è stato effettuato l'accesso e il codice operatore che l'ha compiuto).

j) l sistema deve conservare i dati sensibili (inerenti lo stato di salute e la vita sessuale) in ambenti separati dagli altri dati personali; devono, inoltre, essere determinati criteri per la cifratura dei dati sensibili (attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o data base), al fine di rendere gli stessi intellegibili.

k) Deve essere prevista una procedura di trasmissione sicura delle informazioni e consultazione diretta da remoto e in modo sicuro dei dati personali:

- prevedere, per ogni applicazione e/o sito web (comprese eventuali API), l'utilizzo di protocolli di comunicazione sicura quali TLS (Transport Layer Security), PFS (Perfect Forward Secrecy) e HSTS (HTTP Strict Transport Security);

- i certificati non devono essere self-signed: la Root CA deve essere un'entità riconosciuta nei maggiori trust store (Apple, NSS, Windows). Ottenere certificati EV se possibile;

- in caso di HSTS preload, assicurarsi di seguire le linee guida contenute in https://hstspreload.org/.

l) Il sistema deve prevedere il login prima dell'utilizzo, se vi è una funzionalità che permette di non dover rieseguire il login ad ogni accesso all'applicazione, è opportuno che non venga immagazzinato nel dispositivo alcun tipo di credenziale dell'utente: il sistema deve essere dotato di adeguati metodi di autenticazione che consentano di salvare in maniera sicura all'interno del dispositivo solo un token (come nel caso di OAuth 2.0). Nel caso in cui il salvataggio della password fosse obbligatorio, deve demandare la gestione del salvataggio della password al sistema operativo.

## 1) LINEE GUIDA DI DATA PROTECTION BY DESIGN PER LA TUTELA DELLA DIGNITÀ DEL PAZIENTE

- All'interno dell'ospedale i percorsi devono essere studiati in modo da separare l'accesso alle degenze da quello alle attività ambulatoriali.

- Prevedere la disposizione di apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento dei dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute, accettazione ricoveri ecc…) opportunamente segnalate con cartelli, avvisi ecc.

- Nei reparti in cui ci sono pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è doverosa una particolare attenzione al rispetto della dignità degli stessi, anche per effetto di specifici obblighi di legge o regolamento (in riferimento a pazienti sieropositivi o affetti da infezione HIV, all'interruzione di gravidanza, o a persone offerse da atti di violenza sessuale ecc..). In particolare, nei reparti di rianimazione
devono essere adottati accorgimenti, anche provvisori (es. paraventi) che delimitino la visibilità dell'interessato/paziente durante l'ora di visita ai soli familiari e conoscenti.

- Devono essere previste all'interno dei locali delle strutture sanitarie, nell'erogare le prestazioni sanitarie o nell'espletamento degli adempimenti amministrativi che richiedono un periodo di attesa (es. analisi cliniche; accettazione ecc..); soluzioni che implicano un ordine di precedenza e di chiamata degli interessati, che prescinda dalla loro individuazione nominativa (attribuendo loro un codice alfanumerico fornito al momento dell'accettazione o della prenotazione). Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia della chiamata non nominativa dell'interessato (es. in funzione di particolari caratteristiche legate ad uno stato di disabilità), possono essere utilizzati altri accorgimenti equivalenti (es. un contatto privato col paziente).

Per le prestazioni di Pronto soccorso: notizia o conferma ai soli terzi legittimati, valutate le diverse circostanze del caso e accertata l'identità avvalendosi anche di elementi desunti dall'interessato. In ogni caso, è possibile comunicare informazioni solo sulla circostanza che è in atto o si è svolta una prestazione di PS.

Dislocazione dei pazienti nei reparti: rispettare eventuale richiesta che la presenza non sia data neanche ai terzi legittimati.

Correlazione tra paziente e reparto/struttura: prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza dello stato di salute del paziente attraverso la semplice correlazione tra sua identità e indicazione della struttura/reparto presso cui è ricoverato

# ALLEGATI

## K. (ESTRATTO DEL) QUESTIONARIO TRATTAMENTI DIPENDENTI



Ottobre 2017

QUESTIONARIO DI MAPPATURA DEI TRATTAMENTI DEI DIPEDENTI

Il presente questionario è stato redatto alla luce dell'Opinione 2/2017 "*data processing at work*" del Gruppo di Lavoro di Articolo 29 e ha lo scopo di verificare la presenza di eventuali trattamenti dei dati personali dei dipendenti che richiedono maggiori

**Per facilitare la compilazione del questionario, la colonna D è dotata di un menu a tendina con risposta multipla (SI/NO).**

Se si risponde "NO" alla Colonna D si passa alle righe successive; se la risposta è "SI" è necessario procedere a compilare le colonne F,G e (anch'esse con menu a tendina a risposta multipla). La colonna "H" deve contenere il tipo di dati raccolti (es. Indirizzo IP, nome e cognome, dati del veicolo, dello smartphone ecc.) La colonna "I" invece serve al compilatore per fornire eventuali dettagli che possono essere utili a comprendere l'attività svolta.

| ID | Attività/Trattamento | Descrizione | Svolgete questa attività?(risposta multipla) | Eventuali misure da adottare | Adottate queste misure? (risposta multipla) | Tipi di dati raccolti | Eventuale fornitore esterno | Commenti |
|---|---|---|---|---|---|---|---|---|
| 1 | Strumenti per la prevenzione della perdita di dati (Data Loss Prevention "DLP") | Controllo delle comunicazioni in uscita allo scopo di individuare eventuali violazioni di dati personali o di altre policy aziendali (es.: comunicazione all'esterno di informazioni strategiche aziendali) | SI | Predisposizione di un Wifi gratuito o di dispositivi o terminali autonomi per consentire un legittimo utilizzo privato di alcune strutture di lavoro; | SI | | | |
| | | | | Valutazione periodica sulle attività di monitoraggio per valutare se esistano mezzi meno invasivi per raggiungere il medesimo scopo; | NO | | ... | |
| | | | | Eseguire test di proporzionalità del monitoraggio per valutare se l'elaborazione dei dati in questione sia necessaria per conseguire legittimi obiettivi del datore di lavoro ed eventualmente adottare misure per garantire che la violazione della vita privata e la segretezza delle comunicazioni siano limitate al minimo | | | ... | |
| | | | | | | | | |