REGIONE DEL VENETO
ULSS8 BERICA

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it

www.aulss8.veneto.it

Applicazione del principio di Privacy by Design
e Privacy by Default

Linee guida metodologiche

trasmesse da AZIENDA ZERO

(nota 17.12.2018 prot. 16336) come recepite da U.L.SS. n. 8 Berica

(con apposito atto deliberativo)

INDICE

1. Premessa di carattere organizzativo e metodologico 3
2. Introduzione e ambito di applicazione 3
3. Definizioni 3
4. Destinatari 4
5. Ruoli, Responsabilità e Interazioni 5
6. Attività operative 5
6.1. Mappatura preliminare 5
6.2. Verifica dell'applicabilità dei principi di Privacy by Design e Privacy by Default 5
6.3. Applicazione dei Principi di Privacy by Design e by Default 6
6.4. Modifica o introduzione di un trattamento 6
6.5. Archiviazione della documentazione 6
7. Modifiche al presente documento 6

1. Premessa di carattere organizzativo e metodologico

Ogniqualvolta nel presente documento, a seguito di specifico riferimento normativo, sia indicato quale soggetto il **"Titolare del trattamento"** si faccia riferimento, per lo svolgimento dei diversi adempimenti, al soggetto e/o alla struttura aziendale individuata dal Titolare del trattamento *ratione materiae* ed in base all'organizzazione dettata dall'Atto Aziendale, così come riportato nella tabella di cui al paragrafo 5 *"Ruoli e Responsabilità"; tabella* che dovrà essere quindi completata, da ciascuna Azienda, tenendo conto del proprio, peculiare assetto organizzativo, nonché delle eventuali deliberazioni aziendali già assunte in materia di "privacy europea" per far fronte agli obblighi di cui al GDPR.

Ciò detto, al fine di applicare efficacemente le presenti linee guida, ciascuna Azienda, nel caso in cui non lo avesse già fatto, individuerà preliminarmente le strutture aziendali che dovranno concorrere all'attuazione degli adempimenti oggetto del presente documento, in ragione della natura degli adempimenti medesimi *(a titolo esemplificativo e non esaustivo: verranno distinti gli obblighi di carattere giuridico da quelli di carattere tecnologico ed informatico, piuttosto che da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione, etc..).*

Al fine di dare attuazione alle suesposte indicazioni di Azienda Zero, questa U.L.SS. n. 8 ha approvato l'atto deliberativo del direttore generale ad oggetto: ***"Privacy europea: approvazione del nuovo PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE all'interno dell'ULSS n. 8 Berica al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR"***.

Secondo il *"Piano operativo"* anzidetto e per quanto concerne l'applicazione delle presenti Linee Guida, la struttura aziendale competente è la **UOC Servizi Tecnici e Patrimoniali e sue UOS dell'area informatica (Sistemi Informativi, Reti e Telecomunicazioni, Ingegneria Clinica)** al quale sono stati assegnati compiti e interazioni precisamente riportati nell'anzidetto *"Piano operativo"* a cui si fa espresso ed integrale rinvio.

2. Introduzione e ambito di applicazione

La presente procedura definisce le linee di comportamento, i ruoli, le responsabilità e le tempistiche da porre in essere nel garantire che ciascun trattamento sia configurato prevedendo, fin dalla sua origine, le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento (UE) 679/2016 (GDPR), relativo alla protezione dei dati personali, alla libera circolazione degli stessi e alla tutela dei diritti e delle libertà degli Interessati, tenendo conto del contesto complessivo in cui il trattamento si colloca e delle finalità, nonché dei rischi correlati.

Nello specifico, essa è volta a garantire l'applicazione dei principi di *Privacy by Design e Privacy by Default*, ossia di protezione dei dati personali fin dalla progettazione e protezione degli stessi per impostazione predefinita.

2.1. Riferimenti

La procedura è stata redatta tenendo in considerazione i requisiti regolamentari di cui Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito Regolamento), con specifico riferimento all'articolo 25.

3. Definizioni

Titolare del trattamento (Art. 4, n. 7, del Regolamento): 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 di 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 del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento (Art. 4, n. 8, del Regolamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Interessato: la persona fisica identificata o identificabile **(Art. 4, n. 1, del Regolamento)** a cui si riferisce il dato personale oggetto di trattamento.

Dato personale (Art. 4, n. 1, del Regolamento): 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.

Trattamento (Art. 4, n. 2, del Regolamento): 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.

Principio di Privacy By Design e By Default (Art. 25 del Regolamento)

Trattasi del principio introdotto dall'art. 25 del Regolamento, ove si prevede che "*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.*
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.
Un meccanismo di certificazione approvato ai sensi dell'art. 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo".

Responsabile della Protezione dei Dati (RPD): la persona fisica (o giuridica) nominata ai sensi dell'art. 37 del Regolamento, che svolge la propria attività ai sensi degli articoli 37, 38 e 39 del Regolamento medesimo o di altre disposizioni ivi contenute. Ai sensi del Decreto commissariale di Azienda Zero n. 157/2018, ad oggi, risulta nominato un unico RPD (persona fisica) per le Aziende SSR del Veneto.

4. Destinatari

I destinatari della procedura sono tutti i dipendenti e collaboratori autorizzati al trattamento dei dati.

5. Ruoli, Responsabilità e Interazioni

Come già delineato all'articolo n. 1, al fine di dare attuazione alle indicazioni di Azienda Zero, questa U.L.SS. n. 8 ha approvato l'atto deliberativo del direttore generale ad oggetto: ***"Privacy europea: approvazione del nuovo PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE all'interno dell'ULSS n. 8 Berica al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR"***.

Secondo il *"Piano operativo"* anzidetto e per quanto concerne l'applicazione delle presenti Linee Guida, la struttura aziendale competente è la **UOC Servizi Tecnici e Patrimoniali e sue UOS dell'area informatica** (**Sistemi Informativi, Reti e Telecomunicazioni, Ingegneria Clinica**), alla quale sono stati assegnati compiti e interazioni precisamente riportati nell'anzidetto *"Piano operativo"* a cui si fa espresso ed integrale rinvio.

6. Attività operative

Le fasi di attività connesse alla gestione la corretta applicazione dei principi di *Privacy by Design e Privacy by Default*, si sostanziano in:

1. Mappatura preliminare dei trattamenti eseguiti, delle tipologie di dati trattati e dei soggetti che svolgono operazioni di trattamento
2. Verifica dell'applicabilità dei principi al trattamento
3. Applicazione dei principi al trattamento
4. Modifica o introduzione di un trattamento
5. Archivio della documentazione

6.1. Mappatura preliminare

Preliminare a qualsiasi ulteriore azione è la mappatura dei trattamenti eseguiti, delle tipologie di dati trattati e dei soggetti coinvolti nelle operazioni di trattamento, effettuata dal Titolare del trattamento, anche in sede di predisposizione del ***"Registro elettronico delle attività di trattamento".***
Tale mappatura permette di ricostruire i flussi di trattamento e così di poter fruire di informazioni utili per la migliore applicazione dei principi in oggetto.
La mappatura può avvenire mediante interrogazione aziendale (interviste, audit, ricostruzioni documentali etc.), analisi diretta, consultazione dei ruoli direttivi, compilazione di questionari e con ogni altro mezzo sia idoneo a descrivere lo stato di fatto attuale in cui versano le operazioni di trattamento in seno al Titolare.

6.2. Verifica dell'applicabilità dei principi di Privacy by Design e Privacy by Default

Il Titolare del trattamento verifica la coerenza di ciascun trattamento aziendale ai principi *Privacy by Design* e *Privacy by Default,* in relazione ai singoli ambiti di applicazione del GDPR,

6.3. Applicazione dei Principi di Privacy by Design e by Default

Ogni qualvolta sia previsto lo sviluppo di un **nuovo processo/servizio/strumento** o una modifica dello stesso (di finalità), **preliminarmente** il Titolare del trattamento applica i principi di privacy by design e by default al fine di:

- individuare i dati personali che saranno oggetto di trattamento;
- limitare la raccolta dei dati esclusivamente a quei dati personali realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di minimizzazione dei dati;
- determinare, sin dall'origine, il periodo di conservazione dei dati; tale periodo è determinato sulla base della durata del trattamento previsto, nonché tenendo conto di eventuali obblighi imposti da norme prevalenti. Qualora fosse impossibile determinare un periodo di conservazione definito, è necessario indicare i criteri adottati per definire i tempi di conservazione;
- individuare i dipendenti e/o collaboratori e/o altri soggetti terzi che, per lo svolgimento delle rispettive attività, avranno accesso ai dati personali, al fine di provvedere alla formalizzazione di appositi documenti di nomina, a seconda del caso, a Responsabile del trattamento o a Incaricati del trattamento;
- implementare specifici soluzioni, in ottemperanza ai requisiti per la protezione dei dati personali, che possano impedire o limitare eventi di violazione in seguito ad attacchi informatici esterni o comportamenti illeciti interni; tra questi, a titolo esemplificativo, si cita l'estensiva adozione di tecniche di cifratura delle informazioni "*a riposo*" e in transito, di pseudonimizzazione, di aggregazione dei dati nelle fasi immediatamente successive alla raccolta e sul sistema di origine;
- valutare se il trattamento possa presentare un rischio elevato per i diritti degli interessati.

6.4. Modifica o introduzione di un trattamento

Al termine delle attività sopra descritte, il Titolare del trattamento redige una relazione contenente indicazioni specifiche in merito alle valutazioni effettuate, specificando le eventuali misure tecniche e organizzative identificate come necessarie nella fase di definizione dei principi di *Privacy by Design* e *by Default*.
Il Titolare del trattamento trasmette per conoscenza al RPD la suindicata relazione al fine di ottenerne il parere (non vincolante), laddove necessario e comunque alle condizioni previste dal Regolamento di funzionamento del RPD.

6.5. Archiviazione della documentazione

Il Titolare del trattamento archivia la documentazione e la relazione contenente gli esiti della valutazione finale.

6.6. Checklist Controlli Sicurezza e by DD

E' prodotto in allegato il modello di checklist di cui si tratta.

7. Modifiche al presente documento

Eventuali modifiche al presente documento avranno efficacia dal momento della loro pubblicazione.

***

Allegato 1

Applicazione del principio di Privacy by Design e Privacy by Default

Checklist Controlli Sicurezza e by DD

CHECKLIST SICUREZZA

	Esposizione dati	-	Indicare "SI" se l'attività di change prevede l'esposizione su internet/mobile database di dati personali e/o sensibili quali nome-cognome, password, firme, email, numeri di telefono, etc.
	Piattaforma	-	Indicare se l'applicazione è di proprietà o meno; e se sussistono o sono previste attività di customizzazione
	Tipologia utenti	-	Indicare la tipologia di utenti utilizzatori dell'applicazione
	Ambiente di deploy	[●]	Indicare gli ambienti in cui è installata l'applicazione: Sviluppo, Test, Produzione.
	Linguaggio di programmazione	[●]	Indicare il linguaggio di programmazione in cui è sviluppata l'applicazione
	Detenzione del codice sorgente	-	Indicare "SI" se si possiedono fisicamente i codici sorgente dell'applicazione
	Locazione del codice sorgente	[●]	Indicare il prodotto di versioning sul quale è detenuto il codice sorgente dell'applicazione
	Installazione	-	Indicare se si tratta di un'applicazione client o server
	Interfaccia utente	-	Indicare la tipologia di interfaccia utenti utilizzata dall'applicazione
	Sistema di autenticazione	-	Indicare il sistema di autenticazione utilizzato dall'applicazione
	Sistema di profilazione	-	Indicare il sistema di profilazione utilizzato dall'applicazione
	Certificazioni	-	Indicare la certificazione cui è soggetta l'applicazione; Indicare "Nessuna" qualora l'applicazione non sia soggetta ad alcuna certificazione
	Cifratura database	-	Indicare "SI" se il database utilizzato è protetto da procedure di cifratura
	Anonimizzazione/Pseudonimizzazione dati	-	Indicare "SI" se i dati sono protetti da procedure di anonimizzazione/pseudonimizzazione
Terze Parti	Applicazione di Terze Parti?	-	Indicare "SI" se l'applicazione è comprata da un Fornitore
	Vendor	[●]	SE PRESENTE/PREVISTO, indicare il vendor da cui è stata acquistata l'applicazione
	Support Vendor	[●]	SE PRESENTE/PREVISTO, indicare il fornitore che fa manutenzione dell'applicazione
	Trasferimento dati verso Terze Parti	-	SE PRESENTE/PREVISTO, indicare "SI" se il trasferimento dei dati viene effettuato al di fuori del sistema informativo CLIENTE
	Traferimento dati UE/Extra UE	-	SE PRESENTE/PREVISTO, indicare se il trasferimento dei dati viene effettuato in territorio UE o Extra UE

CHECKLIST PRIVACY BY DESIGN

Responsabile Esterno del Trattamento	Presenza di Responsabile del Trattamento	-	SE GIA' PRESENTE/SELEZIONATO, indicare "SI" se il Fornitore effettua trattamento di dati personali
	Responsabile del Trattamento UE/Extra UE	-	SE GIA' PRESENTE/SELEZIONATO, indicare se il Responsabile Esterno è collocato in territorio UE o Extra UE
	Trasferimento dati UE/Extra UE	-	SE NOTO, indicare se il trasferimento di dati personali avviene in territorio UE o Extra UE
	Denominazione/Ragione Sociale Responsabile del Trattamento	[●]	Indicare la denominazione del Responsabile Esterno
Titolari Autonomi	Presenza di comunicazione a Titolari Autonomi	-	SE GIA' PRESENTE/PREVISTO, indicare "SI" se viene effettuato il trasferimento di dati personali verso Titolari Autonomi
	UE/Extra UE	-	SE GIA' PRESENTE/PREVISTO, indicare se il Titolare Autonomo è collocato in territorio UE o Extra UE
	Trasferimento Dati UE/Extra UE	-	SE NOTO, indicare se il trasferimento di dati personali avviene in territorio UE o Extra UE
	Denominazione/Ragione Sociale	[●]	Indicare la denomiazione Sociale del Titolare Autonomo
Classificazione tipologia dati	DATI PERSONALI	-	Indicare "SI" se il trattamento prevede l'impiego di dati comuni come per es. nome, cognome, data di nascita, residenza, domicilio
	Finanziari / Patrimoniali (cons. 75)	-	Indicare "SI" se il trattamento prevede l'impiego di dati economico finanziari come i dati relativi al reddito, movimenti di conti corrente, saldi patrimoniali, movimenti titoli ecc.
	Categorie particolari di dati personali (art. 9)	-	Indicare "SI" se il trattamento prevede l'impiego di dati c.d. sensibili quali origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita o orientamento sessuale
	DATI videosorveglianza		
	Dati personali relativi a condanne penali e reati (art. 10)	-	Indicare "SI" se il trattamento prevede l'impiego di dati relative a condanne penali o altri tipo di reati
Privacy by default	Quantità di dati raccolti	-	Indicare "SI" se la qualità di dati che si intende coinvolgere nel trattamento è la minima sufficiente per l'esecuzione
	Diritto di accesso	[●]	Indicare il sistema di autenticazione utilizzato/da utilizzare