ORIGINALE

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 115 del 28/02/2019

Il Direttore Generale dell'Azienda U.L.S.S. n. 9 SCALIGERA, dott. Pietro Girardi, nominato con D.P.G.R.V. n. 196 del 30/12/2015 e confermato con D.P.G.R.V. n. 164 del 30/12/2016, coadiuvato dai Direttori:

- dott. Giuseppe Cenci Direttore Amministrativo
- dr.ssa Denise Signorelli Direttore Sanitario
- dott. Raffaele Grottola Direttore dei Servizi Socio-Sanitari

ha adottato in data odierna la presente deliberazione:

OGGETTO

REGOLAMENTO (UE) 2016/679 (PRIVACY EUROPEA): PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - LINEE GUIDA AZIENDA ZERO.

Note per la trasparenza:Regolamento (UE) 2016/679 (Privacy Europea): Piano operativo delle competenze in materia di protezione dei dati personali - linee guida Azienda Zero.

Il Proponente: Il Direttore UOC Affari Generali F.TO Dott. Franco Margonari

DELIBERAZIONE DEL DIRETTORE GENERALE N. 115 DEL 28/02/2019

Il Direttore della U.O.C. Affari Generali, riferisce:

In data 25 maggio 2018 ha trovato diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo (n. 2016/679) sulla privacy (noto anche come "GDPR"), approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il principio cardine introdotto dal nuovo Regolamento Europeo è quello della "responsabilizzazione" (*accountability* nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate ed efficaci in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative che siano concretamente dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o *compliance* nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE, così da poterne dare conto, in qualsiasi momento, verso l'esterno (il termine *accountability*, infatti, rinvia letteralmente al concetto di "resa di conto").

Questa Azienda, nella persona del Direttore Generale, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* ed alla *compliance, inoltre c*on deliberazioni n. 340 del 17.05.2018 e 342 del 24.05.2018, questa Azienda, rispettivamente, ha deliberato "*L'Adesione al progetto "supporto per l'adeguamento al GDPR e attività per l'espletamento del ruolo di responsabile della protezione dei dati (RPD) unico per tutte le Aziende sanitarie del Veneto" da parte dell'AziendaUlss9 Scaligera e stipula della relativa convenzione"* e la *"designazione del Responsabile della Protezione dei dati per l'Azienda Ulss9 Scaligera";*

Azienda Zero (ente di governance della sanità veneta), al fine di fornire linee guida alle aziende in materia di protezione dei dati, agevolando in tal modo l'adempimento dei numerosi adempimenti e uniformando i relativi adempimenti documentali, ha formato un gruppo di lavoro interaziendale specifico, i cui lavori sono stati trasmessi alle Aziende;

Da ultimo, Azienda Zero, con nota del 17 dicembre 2018 (prot. 16336) ha trasmesso a tutte le aziende sanitarie ed ospedaliere della Regione Veneto le nuove "Linee Guida metodologiche e documentali" in materia di privacy europea, elaborate dal Gruppo di lavoro interaziendale coadiuvato dal *Board* del Responsabile della protezione dei dati (RPD) in collaborazione con il Consorzio Arsenàl.

Dette "Linee Guida" hanno lo scopo di favorire, in modo omogeneo, l'applicazione dei complessi adempimenti previsti dal GDPR presso le diverse realtà sanitarie dell'intero territorio regionale.

Il Proponente: Il Direttore UOC Affari Generali F.TO Dott. Franco Margonari

DELIBERAZIONE DEL DIRETTORE GENERALE N. 115 DEL 28/02/2019

Gli adempimenti (con relative Linee guida metodologiche e documentali di Azienda Zero) sono i seguenti:

1. *Revisione e monitoraggio dell'apparato giuridico e documentale*
2. *Implementazione del Registro elettronico delle attività di trattamento*
3. *Garanzia dei diritti degli interessati e gestione istanze in materia di privacy*
4. *Gestione del Risk Assessment e del Data Protection Impact Assessment*
5. *Applicazione del principio di Privacy by Design e Privacy by Default*
6. *Valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni (Data Breach)*

In tutte le Linee Guida licenziate da Azienda Zero si stabilisce espressamente quanto segue:
" (...) 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 G.D.P.R.
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...) (….)";

Ottemperando alle indicazioni di Azienda Zero e sulla base delle funzioni attribuite *ratione materiae* dall'Atto Aziendale alle diverse strutture dell'Azienda, questa UOC Affari Generali ha quindi predisposto un Piano operativo di distribuzione delle competenze all'interno di questa Azienda, al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR;

Si evidenzia che il contenuto del "Piano" di cui si tratta è stato condiviso dalle UOC Affari Generali, UOC Internal Auditing e UOS Sistemi Informativi;

Premesso quanto sopra, si propone di approvare, quale allegato alla presente deliberazione, per formarne parte integrante e sostanziale, il *"Piano operativo delle competenze in materia di protezione dei dati personali",* affidando alle strutture individuate dal medesimo Piano, il compito di farsi carico dell'attuazione degli adempimenti in parola.

Il Proponente: Il Direttore UOC Affari Generali F.TO Dott. Franco Margonari

Di conseguenza, si propone anche di approvare, quali documenti allegati a questa deliberazione, per formarne parte integrante e sostanziale, il testo delle "Linee Guida metodologiche" di Azienda Zero, adattate alle previsioni del "Piano" anzidetto e contenenti i riferimenti del caso a questa Azienda, in luogo di quelli generici contenuti nel testo pervenuto da Azienda Zero.

Infine, come previsto espressamente dal "Piano operativo", che funge anche da strumento di programmazione strategica dell'attività a lungo termine, si propone di rinviare a successive, apposite deliberazioni, l'approvazione della nuova modulistica (di carattere giuridico e contrattuale) formulata da Azienda Zero, nonché i disciplinari tecnici e/o i regolamenti aziendali che, per ciascun adempimento previsto, potranno disciplinare in modo maggiormente dettagliato e analitico i contenuti (per fasi) del lavoro e la distribuzione dei compiti tra le diverse strutture, implementando, a tale scopo, l'apposita applicazione contenuta nel software denominato "DATA PROTECTION MANAGER" (DPM);

Propone l'adozione del provvedimento sotto riportato.

IL DIRETTORE GENERALE

Vista l'attestazione del Responsabile dell'avvenuta regolare istruttoria della pratica in relazione sia alla sua compatibilità con la vigente legislazione nazionale e regionale, sia alla sua conformità alle direttive e regolamentazione aziendali;

Acquisito agli atti il parere favorevole del Direttore Sanitario, del Direttore Amministrativo e del Direttore dei Servizi Socio-Sanitari per quanto di rispettiva competenza;

DELIBERA

1. di approvare, quale documento allegato alla presente deliberazione, quale sua parte integrante e sostanziale, il "*Piano operativo delle competenze in materia di protezione dei dati personali",* affidando alle strutture individuate dal medesimo "Piano", il compito di farsi carico dell'attuazione degli adempimenti ivi prescritti;

2. di approvare le quattro "Linee Guida metodologiche" *di* Azienda Zero *(Gestione diritti degli interessati, Risk Assessment e PIA, Privacy by design e by default, Valutazione incidenti di sicurezza e Data Breach),* adattate alle previsioni del "Piano" aziendale citato al punto n. 1 e contenenti i riferimenti del caso a questa Azienda, in luogo di quelli generici contenuti nel testo pervenuto da Azienda Zero, quali documenti allegati alla presente deliberazione per formarne parte integrante e sostanziale;

DELIBERAZIONE DEL DIRETTORE GENERALE N. 115 DEL 28/02/2019

3. di rinviare, come previsto dal "Piano operativo" che funge anche da strumento di programmazione strategica dell'attività a lungo termine, a successive, apposite deliberazioni, l'approvazione della nuova modulistica (di carattere giuridico e contrattuale) formulata da Azienda Zero, nonché i disciplinari tecnici e/o i regolamenti aziendali che, per ciascun adempimento previsto, potranno disciplinare in modo maggiormente dettagliato e analitico i contenuti (per fasi) del lavoro e la distribuzione dei compiti tra le diverse strutture, implementando, a tale scopo, l'apposita applicazione contenuta nel software denominato "DATA PROTECTION MANAGER" (DPM) ;

4. di incaricare la UOC Affari Generali affinché provveda alla pubblicazione della documentazione di cui ai punti n. 1 e 2 nella sezione dedicata alla "privacy europea" sul sito internet aziendale.

Il Direttore Sanitario	Il Direttore Amministrativo	Il Direttore dei Servizi Socio Sanitari
F.TO dr.ssa Denise Signorelli	F.TO dott. Giuseppe Cenci	F.TO dott. Raffaele Grottola

IL DIRETTORE GENERALE
F.TO dott. Pietro Girardi

Il Proponente: Il Direttore UOC Affari Generali F.TO Dott. Franco Margonari

DELIBERAZIONE DEL DIRETTORE GENERALE N. 115 DEL 28/02/2019

ATTESTAZIONE DI PUBBLICAZIONE E DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva dalla data di adozione.

In data odierna copia della presente deliberazione viene:

- Pubblicata per 15 giorni consecutivi nell'Albo on line, ai sensi e per gli effetti dell'art. 32 – comma 1 – della L. 18.06.2009, n. 69 e s.m.i..
- Trasmessa al Collegio Sindacale, ai sensi dell'art. 10 – comma 5 – della L.R. 14.09.1994, n. 56.

Verona, 11/03/2019

P. il Direttore
UOC Affari Generali
F.TO Sig.ra. Romana Boldrin

TRASMESSA PER L'ESECUZIONE A:

UOC Affari Generali

TRASMESSA PER CONOSCENZA A:

UOC Affari Generali
Tommaso Zanin
Antonietta Ristaino
Sara Gasparini

Il Proponente: Il Direttore UOC Affari Generali F.TO Dott. Franco Margonari

PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(adottato con deliberazione n. ___ del _____)

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Decreto legislativo 10 agosto 2018, n. 101
(Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Linee guida metodologiche di Azienda Zero

PREMESSA
Gli adempimenti (con relative Linee guida metodologiche e documentali di Azienda Zero) sono i seguenti:

1. *Revisione e monitoraggio dell'apparato giuridico e documentale*
2. *Implementazione del Registro elettronico delle attività di trattamento*
3. *Garanzia dei diritti degli interessati e gestione istanze in materia di privacy*
4. *Gestione del Risk Assessment e del Data Protection Impact Assessment*
5. *Applicazione del principio di Privacy by Design e Privacy by Default*
6. *Valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni (Data Breach)*

In tutte le Linee Guida inviate da Azienda Zero si stabilisce espressamente quanto segue:

" (...) 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 G.D.P.R.
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...) (….)"

PIANO OPERATIVO AZIENDALE
Di seguito, ottemperando alle indicazioni di Azienda Zero e sulla base delle funzioni attribuite dall'Atto Aziendale alle diverse strutture dell'Azienda, si stabilisce il seguente affidamento delle competenze per ciascuno dei sei adempimenti sopra citati:

1) Revisione e monitoraggio dell'apparato giuridico e documentale

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * *(Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩ Adempimenti di carattere giuridico, legale ed amministrativo	⇩ Titolare del trattamento *(Direttore Generale)*	⇩ UOC Affari Generali	⇩ Tutte le strutture aziendali coinvolte dagli Affari Generali in ragione dei diversi adempimenti di carattere giuridico e documentale	⇩ Soggetto nominato con delibera n. 342 del 24.05.2018

* Compiti assegnati alla UOC Affari Generali:

- ✓ Promuovere, anche sulla base delle indicazioni di Azienda Zero, le azioni utili a garantire nell'ambito aziendale l'assolvimento dei molteplici obblighi previsti dalla legislazione vigente in materia, sia nazionale che europea;
- ✓ Fornire supporto alle strutture dell'Azienda sugli aspetti di carattere giuridico relativi all'applicazione della privacy europea;
- ✓ Adeguare l'apparato documentale aziendale alle indicazioni di Azienda Zero (vedasi le modulistiche di cui alla nota 17.12.2018 prot. 16336, nonché il materiale inviato con nota del 13.07.2018 prot. 9132), tenendo conto dei precetti di cui al GDPR e delle recenti novità di cui al D.lgs. 101 del 2018 recante misure nazionali di adeguamento al Regolamento Europeo;
- ✓ aggiornare di conseguenza, qualora necessario, il Regolamento aziendale privacy attuativo del GDPR, curando in ogni caso la comunicazione della nuova modulistica a tutte le strutture aziendali interessate, al fine di darne massima pubblicità e diffusione;
- ✓ Predisporre gli atti deliberativi in materia, d'intesa con la Direzione Strategica;
- ✓ Curare la pubblicazione della relativa documentazione nella sezione dedicata alla *"privacy europea"* presente sul sito web aziendale, curandone gli aggiornamenti.

2) Implementazione del Registro elettronico delle attività di trattamento

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * (utilizzando sw DPM) *(Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩ Adempimenti di carattere misto, sia giuridico che tecnologico	⇩ Titolare del trattamento *(Direttore Generale)*	⇩ UOC Affari Generali e UOS Sistemi Informativi	⇩ Tutte le strutture aziendali coinvolte in ragione dei diversi adempimenti di carattere giuridico o informatico	⇩ Soggetto nominato con delibera n. 342 del 24.05.2018

* Compiti assegnati alla UOC Affari Generali e UOS Sistemi Informativi:

- ✓ Completamento del censimento aziendale relativo ai trattamenti, sulla base dello "schema tipo" fornito da Azienda Zero nel mese di maggio 2018, coinvolgendo tutte le strutture aziendali (UOC Affari Generali);
- ✓ Conclusa tale prima fase, avviare la seconda fase dell'attività caricando il contenuto del censimento aziendale nel software "DATA PROTECTION MANAGER - DPM", già acquisito da questa Azienda (UOC Affari Generali);
- ✓ Terza fase: predisporre, utilizzando il citato software "DPM", il nuovo *"Registro elettronico delle attività di trattamento"* dell'ULSS n. 9 Scaligera; registro che potrà essere esibito dal Titolare (Direttore Generale) su richiesta del Responsabile della Protezione dei dati (RPD) aziendale e/o del Garante privacy, come previsto dalla normativa vigente (UOC Affari Generali);
- ✓ rimanere a disposizione di Azienda Zero per fornire, alla medesima Azienda quale ente di governance della sanità veneta, il contenuto dell'intero censimento di cui si tratta, ai fini di ottemperare agli sviluppi di carattere tecnologico ed organizzativo che Azienda Zero riterrà di porre in essere nell'ambito della rete regionale di cui fanno parte tutte le aziende sanitarie ed ospedaliere del Veneto (UOC Affari Generali);
- ✓ comunicare, alle macro strutture e alle strutture dell'Azienda che hanno già predisposto il censimento di cui in premessa, le modalità per effettuare gli eventuali, futuri aggiornamenti delle informazioni già censite, così da garantire il costante aggiornamento, nel tempo, del contenuto del Registro elettronico delle attività di trattamento(UOC Affari Generali e UOS Sistemi Informativi) ;

- ✓ nelle more della completa autonomia in materia di aggiornamento del sw "DPM" da parte dei singoli delegati al trattamento, curare la raccolta ed il caricamento degli eventuali aggiornamenti che perverranno dalle strutture dell'Azienda nel "Registro" di cui si tratta (UOC Affari Generali).

- ✓ garantire la sicurezza informatica delle componenti utilizzate nella fruizione del software utilizzato per l'implementazione del Registro dei Trattamenti, dall'impiego di credenziali individuali e qualificate, alla tracciatura di tutte le attività svolte, alla sicurezza dei collegamenti tra pc e servizio in cloud, alla corretta policy di backup e restore da adottarsi (UOS Sistemi Informativi);

- ✓ curare la compilazione del registro per le informazioni relative agli asset informatici coinvolti e alle misure di sicurezza, sempre relative alla parte IT, applicate nei trattamenti individuati ed elencati nel registro stesso (UOS Sistemi Informativi).

3) Garanzia dei diritti degli interessati e gestione istanze in materia di privacy

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * *(Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩ Adempimenti correlati all'applicazione del GDPR nei confronti dei cittadini-utenti	⇩ Titolare del trattamento *(Direttore Generale)*	⇩ Delegato interno al trattamento dei dati *(UOC – UOSD - UOS in staff, cui si riferisce l'istanza del cittadino)* con il supporto della UOC Affari Generali	⇩ Tutte le strutture aziendali coinvolte, volta per volta, in base all'istanza del cittadino	⇩ Soggetto nominato con delibera n. 342 del 24.05.2018

<u>* Compiti assegnati al Delegato interno al trattamento dei dati:</u>

- ✓ Il Protocollo Generale riceve, protocolla e assegna l'istanza per competenza alla struttura aziendale cui si riferisce l'istanza del cittadino e quindi al Delegato interno del trattamento dei dati (Direttore di UOC - UOSD - UOS in staff, come da nomina del DG);

- ✓ Detto Delegato interno del trattamento dei dati alla cui struttura si riferisce l'istanza del cittadino istruisce e valuta la pratica, fornendo riscontro al cittadino;

- ✓ Usufruisce, in istruttoria, del supporto delle strutture aziendali competenti per gli aspetti di rispettiva competenza *(a titolo esemplificativo: per gli aspetti informatici la UOS Sistemi Informativi e/o UOS Ingegneria Clinica, per gli aspetti clinico-organizzativi la Direzione Medica o la Direzione di Distretto, per gli aspetti relativi alla comunicazione l'URP, per gli aspetti giuridici la UOC Affari Generali, etc…);*

* Compiti di supporto assegnati alla UOC Affari Generali:

- ✓ Fornisce alla struttura aziendale impegnata nell'istruttoria del singolo caso, il necessario supporto di carattere giuridico e normativo;
- ✓
- ✓ Pubblica sul sito internet aziendale, nella sezione dedicata alla "privacy europea", la modulistica aziendale, elaborata sulla base di quella fornita da Azienda Zero, e utilizzabile dal cittadino per far valere i propri diritti in materia di privacy europea;

- ✓ Gestisce l'*archivio interno delle istanze degli interessati* con riferimento alle istanze relative ai diritti previsti dal Regolamento UE n. 2016/679.

4) Gestione del Risk Assessment e del Data Protection Impact Assessment (PIA)

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * (utilizzando sw DPM) *(Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩	⇩	⇩	⇩	⇩
Adempimenti di carattere tecnologico, statistico ed informatico	Titolare del trattamento *(Direttore Generale)*	UOS Sistemi Informativi con UOC Controllo di Gestione e UOC Internal Auditing	Tutte le altre strutture aziendali chiamate a concorrere all'adempimento di cui si tratta	Soggetto nominato con delibera n. 342 del 24.05.2018

* Compiti assegnati a UOS Sistemi Informativi, UOC Controllo di Gestione e UOC Internal Auditing:

- ✓ Gestire l'adempimento di cui si tratta sulla base delle indicazioni contenute nelle Linee Guida metodologiche licenziate da Azienda Zero, utilizzando a tale scopo l'apposita applicazione contenuta nel software "DATA PROTECTION MANAGER" (DPM) di cui sopra;

- ✓ Adottare le scelte tecnologiche, statistiche ed informatiche opportune a realizzare questo adempimento, anche sulla base delle prescrizioni di cui al Documento Programmatico sulla Sicurezza (DPS) e al Piano di Disaster Recovery, tempo per tempo vigenti, nonché, soprattutto, del contenuto dell'implementando Registro elettronico delle attività di trattamento che costituisce, all'interno del sw DPM, lo strumento propedeutico alla produzione, in formato elettronico, della *valutazione di impatto* ("PIA");

- ✓ Redigere, dopo appositi incontri anche con Studio Storti, un Disciplinare tecnico che regoli in modo dettagliato la procedura aziendale relativa al *Data Protection Impact Assessment ("PIA")*: documento che dovrà distinguere in modo specifico gli adempimenti in carico a ciascuna delle tre strutture competenti e sopra citate, stabilendo tempi e modalità per

l'esecuzione della "PIA" nonché stabilendo modalità di formazione e utilizzo dell'applicativo fornito da Studio Storti.
Detto documento dovrà essere condiviso con la Direzione Amministrativa e, se del caso, approvato con atto deliberativo del direttore generale.

5) Applicazione del principio di Privacy by Design e Privacy by Default
(per le componenti tecniche e tecnologiche)

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * (utilizzando sw DPM) *Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩	⇩	⇩	⇩	⇩
Adempimenti di carattere tecnologico, ingegneristico ed informatico	Titolare del trattamento *(Direttore Generale)*	UOS *Sistemi Informativi e UOS Ingegneria Clinica*	I Delegati interni del trattamento dei dati (Direttori UOC- UOSD- UOS in staff, di tutte le aree aziendali) coinvolti volta per volta in base al processo in esame	Soggetto nominato con delibera n. 342 del 24.05.2018

* Compiti assegnati alla UOS Sistemi Informativi e UOS Ingegneria Clinica:

- ✓ Gestire, tenendo conto dei principi esposti nelle Linee Guida metodologiche di Azienda Zero, l'adempimento di cui si tratta anche fornendo le apposite indicazioni tecniche e tecnologiche a tutte le Ditte esterne che collaborano con questa ULSS per la gestione di hardware e software, anche utilizzando il software "DATA PROTECTION MANAGER" (DPM);

- ✓ Adottare, secondo un piano strategico di medio-lungo termine, le scelte tecnologiche ed informatiche necessarie per realizzare questo adempimento;

- ✓ Proporre, se ritenuto necessario, un disciplinare tecnico e/o un regolamento aziendale che disciplini in modo più dettagliato e specifico la procedure aziendali volte a realizzare concretamente l'adempimento in parola: documento che potrà essere adottato con deliberazione del direttore generale.

6) Valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni (Data Breach)

Tipologia di obbligo *(vedasi indicazioni metodologiche di Azienda Zero)*	Responsabilità diretta *(Responsabile)*	Struttura aziendale competente per gli adempimenti * (anche utilizzando sw DPM) *(Preposto)*	Altre strutture aziendali a supporto del Preposto *(Collaboratori)*	RPD *(Supervisore)*
⇩	⇩	⇩	⇩	⇩
Adempimenti relativi all'area dei controlli interni, della *corporate governance,* e della gestione dei rischi per processi	Titolare del trattamento *(Direttore Generale)*	**Delegato interno al trattamento dei dati** *(struttura dell'azienda ove si è verificato il così detto "incidente di sicurezza")* *Istruttoria sull'incidente di sicurezza e valutazione di prima istanza* ⇩ **Nucleo di valutazione ristretto** *Valutazione di seconda istanza* ⇩ **Direttore Generale** *Decisione finale su notifica al Garante*	Tutte le strutture aziendali coinvolte, volta per volta, in base al processo in esame	Soggetto nominato con delibera n. 342 del 24.05.2018

<u>* Compiti assegnati al Delegato interno del trattamento dei dati:</u>

- ✓ Il Delegato interno al trattamento dei dati *(Direttore di UOC - UOSD - UOS in staff, ove è avvenuto l'incidente di sicurezza, cioè la presunta violazione della privacy),* riceve dal Protocollo Generale la segnalazione relativa all'incidente di sicurezza e provvede a istruirla e verificarla acquisendo ogni informazione utile e predisponendo una relazione finale scritta, dalla quale, in ottemperanza a quanto previsto dall'articolo 33 del GDPR Europeo, dovrà risultare una delle tre seguenti conclusioni:
  - **A.** L'incidente di sicurezza non ha comportato alcuna violazione dei dati;
  - **B.** L'incidente di sicurezza ha comportato una violazione dei dati che non presenta un rischio per i diritti e le libertà delle persone fisiche;
  - **C.** L'incidente di sicurezza ha comportato una violazione dei dati che presenta un effettivo e comprovato rischio per i diritti e le libertà delle persone fisiche;

- ✓ Il Delegato interno redige la relazione finale sul caso munendola necessariamente, in qualità di valutatore di prima istanza, di una delle tre conclusioni sopra citate, e trasmette detta relazione al Nucleo di valutazione ristretto dell'Azienda.

- ✓ Detto "Nucleo", che opererà quale organismo di seconda istanza in posizione di indipendenza e terzietà di giudizio, è composto come segue:
  - Direttore Amministrativo, *in qualità di Presidente del Nucleo (o suo delegato);*
  - Responsabile Servizio Internal Auditing *(o suo delegato);*
  - Direttore UOC Affari Generali *(o suo delegato);*
  - Direttore UOS Sistemi Informativi *(o suo delegato);*
  - Direttore della Macro Struttura aziendale (Ospedale, Distretto, Prevenzione) cui afferisce l'unità operativa ove è avvenuta la presunta violazione *(o suo delegato);*

- ✓ Il "Nucleo" potrà confermare la conclusione del Valutatore di prima istanza, oppure formulare una conclusione diversa da quella del Valutatore di prima istanza.

- ✓ Il Nucleo potrà avvalersi del supporto del RPD aziendale nelle valutazioni relative ai casi di particolare complessità, al fine di ricevere indicazioni di indirizzo, e si interfaccia con il medesimo RPD con le modalità previste dalle *"Linee Guida metodologiche"* di Azienda Zero emanate con riferimento alla procedura di Data Breach;

- ✓ Il "Nucleo" darà quindi comunicazione, sull'esito della propria valutazione, sia al Valutatore di prima istanza che al Direttore Generale.

- ✓ Nel solo caso in cui la segnalazione sull'insorgenza dell'incidente di sicurezza provenga dall'esterno dell'azienda (*ad esempio da una istanza o da un reclamo di un cittadino)* il Delegato interno del trattamento dei dati, qualunque sia l'esito della valutazione sull'incidente di sicurezza, concorderà con il Nucleo e con la Direzione Generale il tenore della risposta da fornire al cittadino / utente autore della segnalazione sul presunto *data breach*;

- ✓ Nel solo caso in cui la valutazione finale del "Nucleo" sancisca la conclusione di cui alla lettera "c" dell'art. 33 del GDPR *(c'è stata violazione dei dati che presenta un effettivo e comprovato rischio per i diritti e le libertà delle persone fisiche)*, il Titolare del trattamento dei dati (Direzione Generale) provvederà alla notifica al Garante della privacy con la procedura "DATA PROTECTION MANAGER" (DPM), dandone notizia all'RPD aziendale e agli interessati (nei casi di cui all'art. 34 del GDPR), secondo le modalità che verranno definite in apposito regolamento aziendale;

- ✓ Le risultanze istruttorie di ogni incidente sono, in ogni caso, inserite nel *"Registro elettronico dei data breach*" nell'ambito del software DPM;

- ✓ Si fa espressa riserva, infine, qualora ritenuto necessario per la disciplina di dettaglio della presente procedura, di adottare un apposito Regolamento interno, con atto deliberativo del Direttore Generale.

==========

Procedura per la gestione delle istanze degli Interessati

Linee guida Azienda Zero

(prot. 16336 del 17.12.2018)

INDICE

1. Premessa.

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 Regolamento (UE) 2016/679 (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, da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione,..).

2. Introduzione e ambito di applicazione

La presente procedura definisce le modalità e le misure adottate dall'Azienda Ulss 9 per la gestione delle istanze per l'esercizio dei diritti degli interessati e, nello specifico:

- diritto di accesso ai dati, diritto di rettifica, diritto di cancellazione (*Diritto all'Oblio*), diritto di limitazione di trattamento, diritto alla portabilità, diritto di opposizione, nonchè diritto di non essere sottoposto a decisioni basate unicamente su trattamenti automatizzati, rispettivamente ai sensi degli articoli 15, 16, 17, 18, 20, 21, 22 del Regolamento (UE) 2016/679.

- obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, ai sensi dell'articolo 19 del Regolamento (UE) 2016/679.

L'Azienda Ulss 9 tratta i dati di soggetti interni ed esterni (esempio dipendenti, assistiti e familiari, tirocinanti / stagisti, fornitori, collaboratori a vario titolo, ecc…).

2.1. Riferimenti Normativi

La procedura è stata redatta tenendo in considerazione i requisiti di cui al *Capo III del* Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito anche "Regolamento").

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.

Destinatario (Art. 4, n. 9, del Regolamento): 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.

Diritto di Accesso dell'interessato (Art. 15 del Regolamento)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla

loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Diritto di Rettifica (Art. 16 del Regolamento)
L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla Cancellazione ("*diritto all'oblio*") (Art. 17 del Regolamento)
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, e il titolare del trattamento ha l'obbligo di cancellare, senza ingiustificato ritardo, i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal

diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di Limitazione al trattamento (Art. 18 del Regolamento)
1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (Art. 19 del Regolamento)
Il titolare del trattamento comunica a ciascuno dei destinatari, cui sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'art. 16, dell'art. 17 paragrafo 1 e dell'art. 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla Portabilità dei dati (Art. 20 del Regolamento)
1. L'interessato ha il diritto di ricevere, in un formato strutturato di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti, qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Diritto di Opposizione (Art. 21 del Regolamento)
1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di *marketing* diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali

finalità, compresa la profilazione nella misura in cui sia connessa a tale *marketing* diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di *marketing* diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione, al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Registro delle istanze degli Interessati: documento che elenca le istanze di esercizio dei diritti da parte degli interessati. Il documento è ad uso interno del Titolare ed è tenuto per finalità di archivio e similari.

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, è stato nominato un unico RPD (persona fisica) per tutte le Aziende SSR del Veneto.

4. Destinatari

La procedura è emanata a cura dell'Azienda Ulsss 9 ed è destinata a tutti i dipendenti appositamente incaricati al trattamento di dati personali, coinvolti nella gestione dei diritti degli interessati.

5. Ruoli, Responsabilità e Interazioni

Al fine di dare attuazione alle indicazioni di Azienda Zero, l'Aulss 9 ha adottato la deliberazione con la quale ha approvato il "PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI". Secondo íl citato "Piano operativo", per quanto concerne l'applicazione delle presenti Linee Guida, la competenza in materia è posta in capo al Delegato Interno al trattamento dei dati (Direttore della UOC - UOSD – UOS in staff, cui si riferisce l'istanza del cittadino), supportato dal punto di vista normativo dalla UOC Affari Generali, con le precisazioni previste nel già citato Piano Operativo, a cui si fa espresso ed integrale rinvio.

6. Attività operative

A seguito della ricezione di un'istanza dell'interessato, le fasi di attività in cui si articola il processo di gestione della stessa sono le seguenti:

1. Ricezione dell'istanza;

2. Valutazione dell'istanza;

3. Esercizio del diritto;
4. Risposta e inoltro all'interessato;
5. Archivio della documentazione inerente alla richiesta e la risposta all'interessato;
6. Notifica della richiesta a soggetti terzi.
7. Eventuale parere al RPD, nei soli casi previsti dal Regolamento di funzionamento del RPD.

Si precisa che l'informativa aziendale *privacy* di cui all'art. 13 del GDPR riporta le modalità di esercizio dei diritti affinché l'interessato possa sapere a chi rivolgersi per farli valere. Nello specifico, gli interessati potranno sottoporre le proprie istanze all'Azienda Ulss 9 inviando una comunicazione ad uno dei seguenti seguenti indirizzi: MAIL: protocollo@aulss9.veneto.it PEC protocollo.aulss9@pecveneto.it utilizzando specifica modulistica.

6.1. Ricezione dell'istanza

Quando perviene una richiesta da parte di soggetti interessati per l'esercizio di uno dei diritti ad essi riconosciuti ai sensi del Regolamento, il Titolare del trattamento ha la responsabilità di prendere in carico la richiesta medesima e di coinvolgere, entro tre giorni dalla ricezione, il personale delegato che ne abbia la competenza in relazione all'oggetto dell'istanza. Dovrà, inoltre, procedere all'istruttoria e alla conseguente valutazione della richiesta, garantendo che le tempistiche di risposta siano in linea con i termini previsti dal Regolamento.

Il Titolare del trattamento è, inoltre, tenuto a registrare l'istanza ricevuta nel Registro delle Istanze degli Interessati *(Allegato 2)*).

6.2. Ricezione dell'istanza da parte del RPD

Qualora il RPD, in quanto canale di contatto, ricevesse la segnalazione dall'interessato *ex* art. 38.4 del GDPR *(allegato 3*) provvederà all'inoltro della richiesta al Titolare del trattamento (tramite e-mail) affinché il medesimo provveda all'espletamento della procedura. In tale caso il RPD sarà tenuto informato, per conoscenza, del processo di evasione della richiesta verso l'Interessato.

Il RPD ha, in ogni caso, facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorandone la procedura.

6.3. Valutazione dell'istanza

Il Titolare del trattamento, effettua la valutazione della richiesta presentata dall'interessato e/o inoltrata dal RPD, compresi i profili di infondatezza e di eventuale ripetitività, sulla base dello storico delle istanze ricevute consultando, a tal fine, il Registro delle Istanze degli Interessati di cui al paragrafo 6.1 della presente procedura.

Tale valutazione congiunta ha la finalità di oggettivare e agevolare l'esecuzione delle attività necessarie per evadere la richiesta (ad esempio, identificazione dei dati all'interno dei sistemi gestionali in uso e modifica e/o cancellazione degli stessi sui sistemi).

Qualora dalla valutazione di cui sopra emerga che la richiesta è manifestamente infondata o ripetitiva, il Titolare del trattamento valuterà la sussistenza dei presupposti per richiedere all'interessato un contributo spese ragionevole, basato sui costi amministrativi sostenuti dall'Azienda per ciascuna istanza presentata.

Valuterà, inoltre, l'opportunità di rifiutare di soddisfare la richiesta in presenza di elementi che dimostrino il carattere manifestamente infondato o eccessivo della richiesta medesima, dandone evidenza all'interessato (*allegato 4*).

Nel caso in cui la valutazione dell'istanza sia di particolare complessità o difficoltà, il Titolare del trattamento, potrà chiedere un parere al RPD.

6.4. Esercizio del diritto

Il Titolare del trattamento, provvede a ottemperare a quanto richiesto dall'interessato nell'esercizio degli specifici diritti di cui agli artt. 15-16-17-18-20-21-22

6.5. Risposta all'interessato

Ai sensi dell'art. 12 del Regolamento, il Titolare del trattamento, deve fornire una risposta all'interessato *(allegato 5)* in merito alla richiesta di esercizio di tutti i diritti allo stesso riconosciuti, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta, anche qualora la risposta abbia esito negativo.

Tale termine può essere prorogato di due mesi in casi di particolare complessità o tenuto conto del numero delle richieste ricevute. In caso di estensione del termine di risposta, il Titolare del trattamento è tenuto a comunicare la proroga e a fornire riscontro all'interessato in relazione ai motivi della dilazione delle tempistiche *(allegato 6).*

La risposta deve essere formulata in forma concisa, trasparente e intellegibile e redatta con linguaggio semplice e chiaro.

La modalità di risposta deve tenere in considerazione il canale utilizzato dall'interessato per trasmetterla al Titolare. In particolare, qualora l'interessato abbia presentato richiesta mediante mezzi elettronici, la risposta dovrà essergli fornita, preferibilmente e laddove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Nel caso sia esercitato il diritto di portabilità di cui all'art. 20 del Regolamento, il riscontro dovrà avvenire mediante allegazione in formato elettronico dei dati secondo lo standard esplicato nelle "Linee-guida sul diritto alla portabilità dei dati" WP242, emesse dal Gruppo europeo WP29.

6.6. Archivio della documentazione inerente alla richiesta e la risposta all'interessato

Il Titolare del trattamento ha la responsabilità di archiviare la documentazione relativa alle istanze di esercizio dei diritti da parte degli interessati.

L'archiviazione prevede la suddivisione delle istanze per tipologia di interessato richiedente e la tenuta del Registro delle Istanze debitamente aggiornato.

Il Titolare del trattamento, una volta fornito un riscontro all'interessato richiedente, archivia una copia della comunicazione di risposta, nonché tutta la documentazione pertinente.

6.7. Notifica della richiesta a soggetti terzi

Ai sensi dell'art. 19 del Regolamento il Titolare del trattamento, ha la responsabilità di comunicare a eventuali soggetti terzi a cui i dati personali sono stati trasmessi da parte dell'Azienda, le eventuali rettifiche, cancellazioni e limitazioni del trattamento effettuate a norma degli articoli 16, 17, paragrafo 1, e 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

La comunicazione ai soggetti terzi di cui sopra è effettuata dal Titolare del trattamento, entro il termine di una settimana dal momento dell'intervento di modifica e/o cancellazione effettuato sui dati o di limitazione del trattamento e se ne tiene traccia all'interno del Registro delle Istanze.

Laddove necessario, in casi di particolari difficoltà e/o gravità e, comunque, nel rispetto delle condizioni disciplinate dal Regolamento di funzionamento del RPD, il titolare del trattamento può consultare il RPD affinché esprima un parere sulla questione.

In caso di discordanza di pareri, la decisione finale sull'azione da intraprendere ricade sul Titolare del trattamento, in forza del principio di *accountability*.

In aggiunta, qualora il soggetto interessato ne abbia fatto richiesta, il Titolare del trattamento fornisce evidenza dei soggetti terzi cui sono stati trasmessi i dati personali che lo riguardano.

7. Modulistica associata alla procedura

Allegato 1_modulo per la richiesta di esercizio diritti
Allegato 2_Registro Istanze
Allegato 3_modulo per la segnalazione all'RPD ex art. 38.4 GDPR
Allegato 4_modulo per riposta negativa all'interessato
Allegato 5_modulo per risposta positiva all'interessato
Allegato 6_modulo comunicazione proroga termini all'interessato ex art. 12.3 GDPR

8. Modifiche al presente documento

Eventuali modifiche al presente documento avranno efficacia dalla data della loro pubblicazione e si applicheranno alle nuove istanze presentata dopo tale data, salva diversa disposizione.

==========

Al Direttore Generale dell'Azienda Ulss n. 9 Scaligera
Via Valverde, 42
37122 VERONA

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….

nato/a a…….il……, esercita con la presente richiesta i

seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali
(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;
- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati
(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a)…;

b)….;

c)…;

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati[1]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

- ☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- ☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……..):*
  - ☐ tutti i dati personali forniti al titolare;
  - ☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____

[1] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

4. Opposizione al trattamento
(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto
(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[2]**:**

Via/Piazza
Comune Provincia Codice postale

Oppure e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____

(Luogo e data)

(Firma)

[2] Allegare copia di un documento di riconoscimento

REGISTRO ISTANZE DEGLI INTERESSATI

GESTIONE ISTANZE DEGLI INTERESSATI - REGISTRO ISTANZE - ALL. 2

ID	Soggetto registrante	Data ricezione istanza	Nome e cognome istante	Nome e cognome interessato (se diverso da istante)	Codice Fiscale istante	Codice fiscale interessato (se diverso da istante)	Tipo istanza	Data invio risposta all'istante / interessato	Note
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									

GESTIONE ISTANZE DEGLI INTERESSATI - all. 3

Al Responsabile della Protezione Dati
_____
_____

E-mail: _____

Oggetto: **ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (art. 38.4 Regolamento UE 2016/679 - GDPR)**

Il sottoscritto (Cognome e Nome) _____
Via _____ Comune _____ Provincia (___)
Codice Fiscale _____
Telefono_____ ed e-mail _____
Documento di riconoscimento: tipo documento (carta identità / passaporto / patente di guida): _____ nr. Documento _____ Data di scadenza _____

□ per proprio conto
□ per conto della persona che rappresenta o assiste legalmente
Cognome e Nome _____
Via _____ Comune _____ Provincia (___)
Codice Fiscale _____
Documento riconoscimento:
Tipo documento (carta identità / passaporto / patente di guida): _____ nr. Documento _____ Data di scadenza _____

□ nell'esercizio della responsabilità genitoriale
◊ nell'esercizio della _____ (tutela/curatela/amministrazione di sostegno), in qualità di _____ (tutore/curatore/amministratore di sostegno), in forza del provvedimento del Giudice Tutelare del Tribunale di _____ R.G. numero _____ del ____/___/____
◊ nell'esercizio della seguente qualifica che comporta la rappresentanza o assistenza legale della persona per cui si agisce (indicare la qualifica di chi agisce ed i poteri che ne derivano)
_____
_____
_____
Vista l'informativa per il trattamento dei dati personali di cui agli artt. 13 e/o 14 del GDPR relativamente al trattamento dei seguenti dati personali (indicare i dati personali e/o particolari e il trattamento cui si fa riferimento):
_____
_____
_____
_____
_____

ai sensi dell'art. 38.4 del GDPR segnala la seguente questione inerente al trattamento dei dati personali o altra questione che interessi l'applicazione del GDPR:
_____
_____
_____
_____

_____
_____

ATTENZIONE: LA PRESENTE COSTITUISCE MERA SEGNALAZIONE E NON RAPPRESENTA ESERCIZIO DEI DIRITTI DI CUI AGLI ARTICOLI DA 15 A 22 DEL GDPR.
IN CASO DI ESERCIZIO DEI DIRITTI, UTILIZZARE LA RELATIVA MODULISTICA.

Recapiti per la risposta

Indirizzo postale:
_____
Via/Piazza:
_____
Comune:
_____

Provincia: _____ Codice Postale _____

oppure

e-mail _____Telefax _____

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):
_____
_____
_____
_____
_____
_____

Luogo e data

Firma del segnalante

_____ _____

GESTIONE ISTANZE DEGLI INTERESSATI - all. 4

Egr. sig
_____
_____
_____

Oggetto: Istanza ex art. _____ Regolamento (UE) 2016/679.

Gentile xxx,
In riferimento alla Sua istanza del data richiesta, prot. n. _____, e in conformità a quanto previsto dal Regolamento (UE) 2016/679, si comunica che non è possibile fornire le informazioni da Lei richieste e/o dare seguito alla richiesta di esercizio del/dei diritto/diritti da Lei presentata, per i seguenti motivi:
……
……
……
……
……
……
Si tenga comunque presente che, ai sensi dell'art. 12, comma 4 del Regolamento la SV ha la facoltà di proporre reclamo a un'Autorità di controllo e di proporre ricorso giurisdizionale.
Luogo e data ……

Firma (Titolare del trattamento)

REGIONE DEL VENETO
ULSS9 SCALIGERA

Azienda ULSS 9 - Scaligera

Sede Legale Via Valverde, 42 – 37122 Verona
cod.fisc. e P. IVA 02573090236

GESTIONE ISTANZE DEGLI INTERESSATI - all. 5

Egr. sig
_____
_____
_____

Oggetto: Istanza ex art. _____ Regolamento (UE) 2016/679.

Gentile _____,
In riferimento alla Sua richiesta del data richiesta, prot. n. _____, e in conformità a quanto previsto dal Regolamento (UE) 2016/679, Le comunichiamo:

Diritto di accesso (art. 15 GDPR)

□ La non esistenza dei dati da Lei indicati

□ L'esistenza dei dati da Lei indicati, anche se non ancora registrati.
□ I dati sono accessibili tramite la seguente procedura:
……
□ Estremi identificativi del titolare del trattamento e/o del rappresentante:
……
□ Dati di contatto del responsabile della protezione dei dati:
……
□ Finalità del trattamento dei dati:
……
□ Categorie di dati:
……
□ Destinatari o categorie di destinatari ai quali i dati personali sono stati o potranno essere comunicati o che possono venirne a conoscenza in qualità di responsabili o di incaricati o di rappresentante designato nel territorio dello Stato
……
□ Periodo di conservazione dei dati/criteri per la sua determinazione:
……..
□ Origine dei dati:
……
□ Modalità del trattamento:
……
□ Logica applicata al trattamento effettuato con strumenti elettronici:
……
□ Estremi identificativi del rappresentante del titolare:
……
□ Periodo di conservazione dei dati:
……..

Diritto di rettifica (art. 16 GDPR)

Comunica di avere effettuato le seguenti operazioni

- □ Rettifica dei seguenti dati personali
  - Dati inesatti: …… ……
  - Dati corretti ……..……
- □ Integrazione dei seguenti dati personali
  - Dati incompleti: …… ……
  - Dati corretti ……..……

Diritto alla cancellazione - diritto all'oblio (art. 17 GDPR)

Comunica di aver provveduto alla cancellazione dei seguenti dati personali:
……
……
……
……
……..……..

Diritto di limitazione del trattamento (art. 18 GDPR)
Comunica di aver limitato il trattamento dei seguenti dati:
……
……
……..

Diritto a ricevere la notifica in caso di rettifica o cancellazione o limitazione del trattamento (art. 19 GDPR)
Comunica di aver trasmesso i dati oggetto di rettifica/cancellazione/limitazione di trattamento ai seguenti destinatari:
……
……
……..

Diritto alla portabilità (art. 20 GDPR)
Comunica di aver dato seguito alla richiesta di esercizio del diritto alla portabilità dei seguenti dati:
……
……
……..……..
Disponibili nel seguente formato di file (xls, ecc.)
……..

(Eventuale) e di aver trasferito i medesimi, su richiesta dell'interessato, a:
……..

Diritto di opposizione a taluni trattamenti (art. 21, GDPR)
Comunica che i seguenti dati personali:

……
……
……

- □ non saranno più trattati ai sensi dell'art. 6, p. 1, lettere e) o f)
- □ non saranno più trattati per attività di profilazione ai sensi dell'art. 6, p. 1, lettere e o f)
- □ non saranno più trattati per attività di profilazione per finalità di *marketing* diretto
- □ non saranno più trattati a fini statistici, di ricerca scientifica e/o storica, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico

Diritto di non essere sottoposto a decisione basata unicamente su trattamenti automatizzati, compresa la profilazione (art. 22 GDPR)

- □ Comunica di aver dato seguito alla richiesta di esercizio del diritto di non essere sottoposto a decisione basata unicamente su trattamenti automatizzati, compresa la profilazione

Luogo e data ……

Firma (Titolare del trattamento)

GESTIONE ISTANZE DEGLI INTERESSATI - all. 6

Egr. sig
_____
_____
_____

Oggetto: Istanza ex art. _____ Regolamento (UE) 2016/679. Proroga termine ex art. 12 punto 3

Gentile xxx,

In riferimento alla Sua richiesta del data richiesta, prot. n. _____ si comunica che non è possibile evadere la medesima entro il termine di 1 mese. Tale termine, ai sensi dell'art. 12.3 del Regolamento (UE) 2016/679 (GDPR), sarà pertanto prorogato di:
☐1 mese
☐2 mesi
Motivazione:
……
……
……
……
……

Luogo e data ……

Firma (Titolare del trattamento)

Procedura di Gestione e Notifica Data Breach

Linee guida Azienda Zero

(prot. 16336 del 17.12.2018)

INDICE

1. Premessa

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, o altro).

2. Introduzione e ambito di applicazione

La presente procedura definisce le linee di comportamento da seguire, adottate da Azienda ULSS 9 e indica ruoli, responsabilità, tempistiche e modalità di comunicazione di eventuali violazioni di riservatezza, d'integrità e disponibilità dei dati personali al Garante *privacy* e, ove necessario, a tutti gli Interessati i cui dati personali sono oggetto di violazione.

2.1. Riferimenti normativi

La procedura è redatta tenendo in considerazione i requisiti di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito *Regolamento*) e, nello specifico, gli articoli 33 e 34, nonché le *Guidelines on Personal Data Breach Notification under Regulation* 2016/679 (wp250rev.01) del WP29.

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.

Violazione dei dati personali/Data *breach* (Art. 4. n. 12, del Regolamento): 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**.**

Notifica di una violazione dei dati personali all'Autorità di Controllo: comunicazione del Data *Breach* all'Autorità Garante per la protezione dei dati personali.

Comunicazione di una violazione dei dati personali all'interessato: comunicazione del Data *Breach* al soggetto i cui dati sono stati violati.

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

La procedura è emanata a cura dell'Azienda ULSS 9 a favore di tutti i dipendenti e collaboratori a vario titolo coinvolti nel trattamento di dati personali.

5. Ruoli e responsabilità

Al fine di dare attuazione alle indicazioni di Azienda Zero, l'Aulss 9 ha adottato la deliberazione con la quale ha approvato il "PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI", a cui si fa espresso ed integrale rinvio.

6. Attività operative

Le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (*Data Breach*) si sostanziano in:

1. Rilevazione / Valutazione;
2. Gestione;
3. Notifica al Garante per la protezione dei dati personali;
4. Comunicazione agli Interessati (ove necessario);
5. Pianificazione di Audit Interni;
6. Archivio della documentazione.

6.1. Rilevazione/Valutazione del *Data Breach*

Ai sensi dell'art. 4 n. 12) del Regolamento UE si intende per *Data Breach* 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.

Il Gruppo di Lavoro Articolo 29 per la protezione dei dati, nella *Opinion* 03/2014, ha identificato alcuni tipi di *Data Breach*[1].

In particolare, può trattarsi di:

- "***violazione della riservatezza***": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "***violazione dell'integrità***": in caso di alterazione non autorizzata o accidentale dei dati personali;
- "***perdita della disponibilità***": in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata).

A titolo esemplificativo, si riportano alcuni eventi di violazione dei dati personali per le quali è necessario avviare la procedura:

- perdita o furto di PC o Smartphone aziendali;
- perdita di supporti mobili quali *pen-drive* USB o *hard disk* aziendale;
- perdita di fascicoli cartacei o altra documentazione aziendale;
- invio erroneo di comunicazioni/informazioni verso l'esterno;

[1] Per ulteriori approfondimenti si veda: Gruppo di Lavoro Articolo 29 per la protezione dei dati, Opinion 03/2014.

- attacchi informatici ai sistemi aziendali;
- accesso a dati da parte di persona non autorizzata.
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o sia loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono stati violati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- se sono stati violati dati afferenti alla valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se la violazione afferisce a un numero rilevante di dati;
- se l'evento riguarda il trattamento di dati personali di persone fisiche vulnerabili, in particolare minori.

Qualsiasi persona autorizzata al trattamento in Azienda, ogni qualvolta rilevi un avvenuto o potenziale *Data Breach*, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del trattamento.

La comunicazione al Titolare del trattamento della violazione dei dati personali dovrà pervenire, all'Azienda Ulss 9 inviando una comunicazione ad uno dei seguenti seguenti indirizzi: MAIL: protocollo@aulss9.veneto.it PEC protocollo.aulss9@pecveneto.it utilizzando specifica modulistica.

Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma 2 Regolamento (UE), con le medesime modalità di cui sopra.
Il Titolare del trattamento, avuta notizia dell'avvenuto o potenziale *Data Breach*, avvia l'istruttoria per l'identificazione dell'evento, informando del caso il personale delegato di competenza in relazione alla questione e coinvolgendo eventualmente anche il Referente aziendale ICT.
In questa fase, il Titolare del trattamento ha la possibilità di consultare il RPD per funzioni di indirizzo, utilizzando apposita modulistica *(allegato 1)* e, comunque, nel rispetto delle condizioni disciplinate dal Regolamento di funzionamento del RPD.

Il Titolare del trattamento procede alla compilazione del *Registro Interno delle Violazioni (allegato 2)* indipendentemente dalle notifiche che saranno effettuate all'Autorità di controllo. Tale registro ha la funzione di documentare le valutazioni effettuate circa l'identificazione del *Data Breach*.

6.2. Gestione del *Data Breach*

Il Titolare del trattamento, laddove necessario o opportuno, procede nella gestione del *Data Breach* raccogliendo le informazioni necessarie alla descrizione dell'evento, delle misure tecniche e organizzative analogiche e/o digitali adottate e di quelle di possibile adozione per porre rimedio alla violazione e/o per attenuarne i possibili effetti negativi; ciò al fine di poter procedere nella compilazione della modulistica per la notifica al Garante.

Infine, valuta la possibilità che la violazione presenti un rischio per i diritti e le libertà degli interessati, avvalendosi del supporto del RPD nei casi di particolare complessità, per ricevere indicazioni di indirizzo.
Qualora il Titolare del trattamento dovesse ritenere non opportuno notificare la violazione di riservatezza dei dati, è necessario che le motivazioni sottostanti a tale decisione siano documentate all'interno del sopracitato *Registro Interno delle Violazioni*. A tale proposito, occorrerà descrivere i motivi per cui il Titolare del trattamento ha ritenuto che la violazione non costituisse fattore di rischio per i diritti e le libertà degli individui.

Ai fini della gestione del *Data Breach* occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione;
- l'evento non costituisca un *Data Breach*.

6.3. Notifica al Garante per la protezione dei dati personali

Ai sensi dell'art. 33 del Regolamento, la notifica del *Data Breach* all'Autorità di controllo è sempre obbligatoria, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Alla comunicazione effettuata dal Titolare del trattamento dovrà essere allegata anche dettagliata relazione, comprensiva di tutti gli elementi informativi e delle valutazioni in merito effettuate.

Qualora il Titolare del trattamento ed il RPD (eventualmente consultato) abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali al Garante per la protezione dei dati personali ricadrà unicamente sul Titolare del Trattamento e dovrà essere debitamente motivata.

Laddove, invece, sia rilevato un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento dovrà effettuare la notifica all'Autorità Garante. In particolare, il Titolare del trattamento, utilizzando il *format* e le procedure previste dall'Autorità Garante, dovrà notificare la violazione all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne sia venuto a conoscenza.
Contestualmente è inoltrata dal Titolare del trattamento comunicazione scritta al RPD di avvenuta notifica al Garante, per mettere il medesimo a conoscenza dell'istruttoria in atto.
Qualora la notifica al Garante per la Protezione dei dati personali non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.

Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.
In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.

La mancata collaborazione delle risorse coinvolte assume rilevanza a fini disciplinari.

Ai sensi dell'art. 33 del Regolamento, la notifica all'Autorità di controllo deve contenere almeno i seguenti contenuti:

a) descrizione della natura della violazione dei dati personali, compresi – ove possibile – le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

6.4. Comunicazione agli Interessati

Nel caso in cui la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvede alla comunicazione di detta violazione a tutti gli interessati coinvolti, senza ingiustificato ritardo, dandone comunicazione per conoscenza al RPD.

La comunicazione agli interessati deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

a) la descrizione delle probabili conseguenze della violazione dei dati personali;
b) la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;

c) nome e dati di contatto del RPD.

Ai sensi dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, è necessario procedere a una comunicazione pubblica, ovvero a una misura simile alternativa, tramite la quale gli Interessati sono informati con analoga efficacia.

Nel caso in cui sia il Garante per la protezione dei dati personali a ordinare con provvedimento la comunicazione del *Data Breach* agli interessati, il Titolare del trattamento pone in essere tutte le attività necessarie per ottemperare al provvedimento.

6.5. Pianificazione degli *audit*

Il Titolare del trattamento prevede, all'interno del proprio piano di *audit*, con cadenza almeno biennale, una verifica sulla tenuta del Registro interno delle violazioni e delle segnalazioni di violazione dei *Data Breach*.

6.6. Archiviazione

Il Titolare del trattamento, conclusa la procedura, archivia tutte la documentazione relativa al procedimento, incluse le notifiche trasmesse al Garante per la protezione dei dati personali e agli interessati, nonché il Registro interno delle violazioni debitamente aggiornato. Il RPD potrà accedere al Registro interno delle violazioni in qualsiasi momento.

7. Modulistica allegata alla procedura

Allegato 1_Modulo di richiesta consulenza al RPD
Allegato 2_Registro interno delle violazioni

8. Modifiche al presente documento

Eventuali modifiche al presente documento avranno efficacia dal momento della loro pubblicazione e si applicheranno alle nuove fattispecie di *Data Breach* che si manifesteranno, eventualmente, dopo tale efficacia, salva diversa disposizione.

==========

"Procedura di Gestione e Notifica Data Breach"

Registro Interno delle Violazioni - all. 1

ID	Soggetto registrante	Data segnalazione	Data Inizio Disservizio	Data Fine Disservizio	Durata hh:mm	Descrizione dell'evento	Impatti Verificatisi	Misure di mitigazione del rischio
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

GESTIONE E NOTIFICA DATA BREACH - ALL. 2

Data, Prot.n.

Al Responsabile della Protezione dei Dati
_____
_____

E-mail: _____

Oggetto: Richiesta consulenza al RPD per *Data Breach*

Il sottoscritto …..... in qualità di ……. dell'Azienda Sanitaria ……. contatto telefonico …… e-mail …… fornisce le seguenti indicazioni relative alla presunta violazione dei dati personali, oggetto di consulenza:

QUESITO *(descrizione di alcuni elementi utili alla definizione della risposta):*

Data rilevazione della presunta violazione…….

Natura e tipologia della presunta violazione:
……..
……..
……..

Soggetti coinvolti:
……
……

Informazioni raccolte:
……
……

Azioni sviluppate:
……
……
……

Azioni che il Titolare intenderebbe adottare:
……
……
……

Quesito:
……
……
……

Firma ……

Applicazione del principio di Privacy by Design e Privacy by Default

Linee guida Azienda Zero

(prot. 16336 del 17.12.2018)

INDICE

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,).

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, è stato 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 e responsabilità

Al fine di dare attuazione alle indicazioni di Azienda Zero, l'Aulss 9 ha adottato la deliberazione con la quale ha approvato il "PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI", 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
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.

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

Linee guida metodologiche per la conduzione del *Risk Assessment* e del *Data Protection Impact Assessment*

Linee guida Azienda Zero
(prot. 16336 del 17.12.2018)

INDICE

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.
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, da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione,..)

2 Introduzione e obiettivi del documento

2.1 Introduzione

L'articolo 35 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito GDPR) introduce il concetto di valutazione d'impatto sulla protezione dei dati (in inglese *Data Protection Impact Assessment*, DPIA).

Una valutazione d'impatto sulla protezione dei dati è "*un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli*[1]".

Secondo quanto previsto dall'art. 35, paragrafo 1 del GDPR[2] non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento, ma solo quando il tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento trattamento ***"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*** Inoltre, ai sensi del sopracitato articolo, una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2.2 Obiettivi del documento

Nell'ambito del contesto sopra descritto, il presente documento ha come obiettivo quello di fornire una guida metodologica per lo svolgimento del *Risk Assessment* (analisi del rischio) sui trattamenti posti in essere dall'Azienda Ulss 9, tracciati all'interno del **"Registro delle attività di Trattamento".**

A seguito dell'identificazione dei trattamenti a rischio elevato per i diritti e le libertà degli interessati, il presente documento fornisce, altresì, la guida metodologica per la conduzione del processo di *Data Protection Impact Assessment* su tali trattamenti.

---

[1] WP 248, rev. 01 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679, *Working Party* 29 versione 4/10/2017."

[2] Art. 35.1. "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."

3 Termini e definizioni

Titolare del trattamento (Art. 4, n. 7, del GDPR): 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 GDPR): 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 GDPR)** a cui si riferisce il dato personale oggetto di trattamento.

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

Probabilità: valutazione della frequenza con cui il trattamento è effettuato.

Impatto: indicazione della gravità di un incidente che può compromettere la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa *privacy*.

WP29 (Article 29 Working Party o Gruppo di Lavoro Articolo 29 per la protezione dei dati): il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB)

WP 248, rev. 01: "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018

4 Ambito di applicazione

Ai sensi di quanto disposto dall'art. 35 del GDPR, la valutazione d'impatto sulla protezione dei dati personali è richiesta, in particolare, nei seguenti casi:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il punto 4 del predetto art. 35 prevede, inoltre, che l'autorità di controllo rediga e renda pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1.

In adempimento alla norma sopra citata il Garante per la protezione dei dati personali, con provvedimento n. 467 dell'11.10.2018, pubblicato nella Gazzetta Ufficiale il 19/11/2018 (doc.web n. 9058979) ha individuato l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto come di seguito riportato:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche I trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto

sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Il Garante nel suddetto documento evidenzia, però, che l'elenco non è esaustivo, essendo riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza da parte del Comitato di cui all'art. 68 del GDPR, e che lo stesso è stato predisposto allo scopo di specificare ulteriormente il contenuto ed a complemento dei criteri individuati dal WP248 rev 01 dello stesso, restando fermo l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più criteri individuati dal WP248 rev 01 e che in taluni casi "un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno dei predetti criteri richieda una valutazione d'impatto sulla protezione dei dati" [3]

[3] Nel WP248 rev 01 sono individuati i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato": 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o dati aventi carattere altamente personale; 5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combinazione di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9)

Inoltre, seppure:

- nel documento WP248 rev. 01 il WP29 indichi come non necessaria una valutazione d'impatto sulla protezione dei dati quando:

  - il trattamento non è tale da presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
  - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è già stata svolta una valutazione d'impatto sulla protezione dei dati;
  - le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018, in condizioni specifiche che non sono mutate;

e

- l'art. 35, paragrafo 10 GDPR disponga che "*Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e) (*cioè qualora la base del trattamento sia un obbligo legale o un interesse pubblico, ndr*), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il* trattamento *specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento*",

è vero anche che nei casi in cui non risulti chiara l'obbligatorietà di una valutazione d'impatto sulla protezione dei dati, il WP29 raccomanda di effettuarla ugualmente.

Pertanto si raccomanda di eseguire sempre una valutazione di impatto, sia in quanto non è per lo più noto se una valutazione di impatto generale sia stata eseguita nel contesto dell'adozione della base giuridica di riferimento, sia perché detta valutazione è uno strumento utile in grado di assistere i Titolari del trattamento nella migliore conformazione al GDPR e soprattutto nella migliore dimostrazione dell'accountability, ossia della capacità di dimostrazione di tale conformazione.

5 Rischio *privacy*. Ruoli e responsabilità

La definizione dei ruoli e delle responsabilità dei soggetti coinvolti nelle attività oggetto della presente procedura deve essere effettuata sulla base della struttura organizzativa dell'Azienda sanitaria.

il Titolare svolge la valutazione d'impatto sulla protezione dei dati in collaborazione con il personale di competenza e tramite le strutture aziendali già individuate nel "PIANO OPERATIVO DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" a cui si fa espresso ed integrale rinvio.

Nelle linee guida in materia di DPIA del WP29 si legge, infatti, che "*la valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno*

---

quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto");

dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito".
Ai fini dell'attribuzione di ruoli e responsabilità, si consideri che, ai sensi dell'art. 35, paragrafo 2, del GDPR, è previsto che il Titolare possa consultarsi con il RPD (*quest'ultimo, ai sensi dell'art. 39, paragrafo 1, lettera c, deve sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati*).
A tale proposito, il WP29 ha specificato che "*il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati*"[4].

Sul punto si segnala, inoltre, che il WP29 raccomanda al Titolare del trattamento di consultare il RPD, fra l'altro, sulle seguenti tematiche[5]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne, ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR.

Qualora il Titolare del trattamento non concordi con le indicazioni fornite dal RPD, occorre che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Nel caso in cui il trattamento sia eseguito in tutto o in parte da un Responsabile del trattamento dei dati, quest'ultimo deve assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie, conformemente all'art. 28, paragrafo 3, lettera f).

6 L'attività di Risk Assessment

L'attività di *Risk Assessment* si sviluppa sulla base dei seguenti step metodologici:

Step 1: Definizione del valore di criticità dei trattamenti
Step 2: Identificazione trattamenti critici.

Nei paragrafi successivi è riportato il dettaglio degli step metodologici previsti ai fini dello svolgimento del *Risk Assessment*.

6.1 Definizione del valore di criticità dei trattamenti

La definizione del valore di criticità dei trattamenti è effettuata partendo dalla mappatura dei trattamenti dei dati personali effettuati dall'Azienda e tracciati all'interno del "Registro

[4] *Gruppo di Lavoro Articolo 29 per la protezione dei dati, "Linee guida sui responsabili della protezione dei dati" – 16/IT WP243rev.01, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, pag. 17.*
[5] *Gruppo di Lavoro Articolo 29 per la protezione dei dati, "Linee guida sui responsabili della protezione dei dati" – 16/IT WP243rev.01, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, pag. 23.*

delel attività di Trattamento " aziendale.

Nel dettaglio, il contenuto informativo riguarda gli ambiti:
- ID Trattamento
- Direzione/Unità Organizzativa
- Finalità del trattamento
- Base giuridica del trattamento
- Categorie interessati
- Categorie dati personali
- Categoria destinatari a cui i dati personali sono stati o saranno comunicati
- Termine cancellazione dati
- Applicativo o banca dati (cartaceo o elettronico)
- Misure di sicurezza tecniche ed organizzative
- Trattamento verso paese terzo (se previsto) - Paese o organizzazione a cui si invia
- Trattamento verso paese terzo (se previsto) – Garanzie

Per ognuno dei trattamenti mappati, il Titolare del trattamento procede con la valorizzazione qualitativa (SI; NO) di 24 variabili utili per la definizione del livello di criticità dei trattamenti (rif. Allegato 1).

Tali variabili sono classificate nelle seguenti 7 categorie, corrispondenti alle principali determinanti che contribuiscono all'esposizione al rischio di ciascun trattamento:

1 Trattamento categorie particolari di dati
2 Trattamento dati di minori
3 Trattamento su altre categorie di dati
4 Finalità
5 Coinvolgimento soggetti terzi
6 Infrastruttura
7 Utilizzo *device* e/o supporti removibili

A ognuna delle 24 variabili oggetto di valutazione è associato un peso (rif. Allegato 1), espressione del livello di criticità associato alla variabile stessa sulla base della scala di seguito riportata.

Livelli di criticità delle variabili		
Livello di criticità	**Peso delle variabili**	**Descrizione**
ALTO	3	Variabile che può determinare un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche
MEDIO	2	Variabile che può determinare un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche

BASSO	1	Variabile che può determinare un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti e sulle libertà delle persone fisiche

Il valore di criticità del trattamento è ottenuto come somma del peso delle variabili valorizzate con "Sì".

6.2 Identificazione trattamenti critici

Sulla base del valore di criticità determinato, i trattamenti sono classificati in funzione del rispettivo livello di criticità sulla base dell'applicazione dei *range* di seguito riportati:

Livelli di criticità del trattamento			
Livello di criticità	**Descrizione**	**Range per la determinazione del livello di criticità**	**Descrizione range**
ALTO	Il trattamento determina un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche	∑n: k≥20 V $X_1 \geq 1$	Sono considerati trattamenti a criticità **"Alta"** tutti i trattamenti la cui somma delle variabili è maggiore o uguale a 20, o se il trattamento è caratterizzato dalla presenza di almeno una variabile con livello di criticità "3" [6]
MEDIO	Il trattamento determina un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche	∑n: 10≤k≤19 V $X_2 \geq 2$	Sono considerati trattamenti a criticità **"Media"** tutti i trattamenti la cui somma delle variabili è compresa tra 10 e 19, o se il trattamento è caratterizzato dalla presenza di almeno due variabili con livello di criticità "2"
BASSO	Il trattamento determina un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti e sulle libertà delle persone fisiche	∑n: k<10 V $X_1=0$ $X_2<2$	Sono considerati trattamenti a criticità **"Bassa"** tutti i trattamenti la cui somma delle variabili è minore di 10, o se il trattamento non è caratterizzato dalla presenza di variabili con livello di criticità "3" e dalla presenza di un numero di variabili con livello di criticità "2" inferiore a 2.

[6] Tale criterio, in caso di contrasto, prevale su quello relativo alla somma numerica delle variabili.

Un trattamento è valutato come "critico" nel caso in cui il Livello di Criticità del Trattamento risulti uguale ad "ALTO".
Per i trattamenti critici identificati, il Titolare del trattamento, effettua la valutazione del rischio per i diritti e le libertà delle persone fisiche scaturente dal trattamento nei seguenti due momenti:

- Valutazione del Rischio Inerente sulla base di criteri di impatto e probabilità;
- Valutazione del Rischio Residuo a seguito della valutazione dei controlli posti in essere ai fini della mitigazione del rischio e corrispondenti al sistema di prevenzione e protezione dei dati personali in essere.

7 L'attività di Data Protection Impact Assessment

L'attività di *Data Protection Impact Assessment* (DPIA) si sviluppa sulla base dei seguenti step metodologici:

Step 1: Valutazione del livello di Rischio Inerente
Step 2: Identificazione tipologia di trattamento
Step 3: Valutazione controlli
Step 4: Definizione del livello di Rischio Residuo
Step 5: Identificazione trattamenti rischiosi

Nei paragrafi successivi si riporta il dettaglio degli step metodologici previsti ai fini dello svolgimento del *Data Protection Impact Assessment*.

7.1 Valutazione del livello di Rischio Inerente

Il *Data Protection Impact Assessment* inizia con la valutazione del Rischio Inerente, attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere dall'Azienda per la sua mitigazione, combinando, sulla base di metriche predefinite, le seguenti due dimensioni:

- **Impatto**, ovvero il possibile effetto che la diffusione dei dati potrebbe avere per l'interessato;
- **Probabilità di accadimento,** ovvero la frequenza con cui il trattamento è effettuato.

Il Titolare del trattamento, valuta qualitativamente l'impatto e la probabilità connessi a ciascun trattamento sulla base dell'applicazione di specifiche scale di valutazione (rif. Allegati 2 e 3).

I valori di Impatto e Probabilità attribuiti sono tradotti quantitativamente su una scala da 1 a 4, dove 1 corrisponde al valore minimo (es. Impatto = Trascurabile; Probabilità = Evento raro) e 4 corrisponde al valore massimo (es. Impatto = Massimo; Probabilità = Evento probabile).

Il Rischio Inerente è calcolato quantitativamente come il prodotto tra i valori di Impatto e Probabilità associati a ciascun trattamento in un *range* da 1 a 16[7].[8]

[7] In un'ottica di efficienza operativa la valutazione dei controlli può essere svolta anche solo per i trattamenti il cui valore di Rischio Inerente è maggiore o uguale a 6. I restanti trattamenti sono considerati infatti già a livello Inerente a basso rischio.

[8] Si suggerisce la lettura del documento " Analyse d'impact relative à la protection des donnès : 3. Les bases de connaissance" emesso dalla CNIL, l'Autorità francese per la protezione dei dati (versione in inglese "Privacy Impact Assessment. Knowledge bases")
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf versione francese
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledge bases.pdf versione inglese

7.2 Identificazione tipologia di trattamento

Ai fini della valutazione dei controlli previsti nell'ambito dello Step 3, il trattamento è classificato in funzione delle modalità con cui è svolto, in:

- Cartaceo: trattamento effettuato unicamente in modalità cartacea;
- Elettronico: trattamento effettuato unicamente in modalità elettronica;
- Cartaceo/Elettronico: trattamento effettuato in modalità cartacea ed elettronica.

7.3 Valutazione controlli

In seguito all'identificazione della tipologia di Trattamento (cartaceo, elettronico o cartaceo/elettronico), il Titolare del trattamento, effettua la valutazione dei controlli per i trattamenti in funzione della tipologia identificata:

- **Tipologia di trattamento cartaceo**: valutazione dei seguenti 4 controlli, definiti sulla base delle *best-practice* di *Risk Management* e tenendo conto della Metodologia di *Risk Management* ISO 31001, di seguito riportata:

  1 chiara identificazione di ruoli e responsabilità del controllo;
  2 periodico svolgimento delle attività di controllo;
  3 formale definizione dei controlli/ norme comportamentali in policy/procedure aziendali;
  4 presenza di misure di sicurezza fisiche per la gestione del cartaceo (es. presenza armadi/distruggi documenti).

- **Tipologia di trattamento elettronico**: valutazione di 14 controlli, coincidenti con i domini dello standard ISO/IEC 27001/2013, associati a specifici obiettivi in materia di Sicurezza delle Informazioni (rif. Allegato 4) e di seguito riportati:

  1 politiche per la sicurezza delle informazioni;
  2 organizzazione della sicurezza delle informazioni;
  3 sicurezza delle risorse umane;
  4 gestione degli *asset*;
  5 controllo degli accessi;
  6 crittografia;
  7 sicurezza fisica e ambientale;
  8 sicurezza delle attività operative;
  9 sicurezza delle comunicazioni;
  10 acquisizione, sviluppo e manutenzione dei sistemi;
  11 relazioni con i fornitori;
  12 gestione degli incidenti relative alla sicurezza delle informazioni;
  13 *disaster recovery – business continuity*;
  14 *compliance*.

- **Tipologia di trattamento Cartaceo/Elettronico:** valutazione sia dei controlli per i trattamenti cartacei, che dei controlli definiti per i trattamenti elettronici, per un totale di 18 controlli.

Ogni controllo è valutato quantitativamente sulla base di una scala a tre livelli:

- 0: Controllo nullo/assente;
- 0,5: Controllo parzialmente soddisfatto;
- 1: Controllo totalmente soddisfatto.

Ai fini del calcolo del Livello di Controllo, distintamente per le due tipologie di controlli (per trattamenti elettronici/Per trattamenti cartacei) è associato un peso uniforme.
La valutazione del controllo per ogni trattamento è ottenuta come somma ponderata della valutazione associata a ciascun controllo per il relativo peso.
Ai fini della definizione del livello di Rischio Residuo previsto nello step 4, per i Trattamenti effettuati in modalità Cartaceo/Elettronico è considerata la minore tra le valutazioni del controllo associate.

7.4 Definizione del livello di Rischio Residuo

Il valore del Rischio Residuo per ciascun trattamento è definito a partire dal valore di Rischio Inerente e in considerazione del valore del controllo mediante l'applicazione del seguente algoritmo di calcolo:

$$Valore\ Rischio\ Residuo = Valore\ Rischio\ Inerente * (1 - Valutazione\ Controllo)$$

Il valore ottenuto è successivamente ricondotto a una scala qualitativa ad 8 valori (rif. Allegato 5).

7.5 Identificazione trattamenti rischiosi

In considerazione del livello di Rischio Residuo, i trattamenti sono classificati in:

- **Trattamenti a rischio trascurabile**: trattamenti che presentano un valore del Rischio Residuo minore di 4 (corrispondente ai Livelli Trascurabile / Molto-Basso) e per i quali non è necessario indirizzare azioni di adeguamento;
- **Trattamenti a rischio basso**: trattamenti che presentano un valore del Rischio Residuo minore di 8 e maggiore di 4 (corrispondente ai livelli Basso / Medio-Basso) per i quali non è necessario indirizzare azioni di adeguamento, ma è possibile valutare delle azioni per il miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;
- **Trattamenti a rischio medio**: trattamenti che presentano un valore di Rischio Residuo minore di 12 e maggiore di 8 (corrispondenti ai livelli Medio / Medio Alto), per i quali è consigliato di individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;
- **Trattamenti a rischio alto**: trattamenti che presentano un valore del Rischio Residuo maggiore di 12 (corrispondenti ai livelli Alto / Molto Alto), per i quali è necessario individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio. In questo caso il Titolare del trattamento è obbligato a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento.

8 Consultazione Preventiva

Nel caso in cui la valutazione d'impatto sulla protezione dei dati produca come risultato finale che il trattamento presenta un Rischio Residuo elevato (c.d. Trattamenti a Rischio Alto), anche sulla base dei presidi di controllo in essere, il Titolare del trattamento pone in essere le attività necessarie

a effettuare una c.d. consultazione preventiva con l'Autorità di controllo.

Ai sensi dell'art. 36, paragrafo 3, del GDPR, la richiesta di consultazione inviata dovrà contenere indicazioni almeno relativamente a:

- ove applicabile, le rispettive responsabilità del Titolare del trattamento, di eventuali contitolari e responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- le finalità e mezzi del trattamento previsto;
- le misure e le garanzie previste per la protezione dei diritti e delle libertà degli interessati;
- ove applicabile, i dati del RPD;
- le valutazioni di impatto sulla protezione dei dati dalle quali è risultato un livello di rischio elevato;
- eventuali ulteriori informazioni richieste da parte dell'Autorità di Controllo.

L'Autorità di controllo, entro un termine di otto settimane, al massimo prorogabile di ulteriori sei settimane, fornirà un parere scritto all'interno del quale sarà indicato se ritiene che il trattamento in esame violi i requisiti regolamentari oppure se lo stesso sia in linea con quanto disciplinato dal GDPR.

==========

DPIA - Allegato 1 - Variabili oggetto di valutazione e relativi pesi

#	Variabile	Peso della variabile per la determinazione del livello di criticità del trattamento
1	Dati che rivelano l'origine razziale o etnica	3
2	Dati che rivelano le opinioni politiche	3
3	Dati che rivelano le convinzioni religiose o filosofiche	3
4	Dati che rivelano l'appartenenza sindacale	3
5	Dati genetici	3
6	Dati biometrici	3
7	Dati relativi alla salute (Appartenenza a categoria protetta o info su permessi per malattia o info su permessi per Maternità senza visibilità del referto medico)	2
8	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	3
9	Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	3
10	Profilazione e/o *marketing* su minori	3
11	Trattamento categorie particolari di dati su minori	3
12	Dati di identità per altre finalità	2
13	Carte di Credito / CC Bancari	3
14	Dati di localizzazione	1
15	Dati di Videosorveglianza	3
16	Finalità di *marketing* (invio comunicazioni commerciali)	2
17	Finalità di profilazione	3
18	Presenza di soggetti terzi (fornitori e non) con cui possono essere condivisi i dati	2
19	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Cloud / SaaS)	2
20	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Private Cloud)	1
21	*MS Exchange in Private Cloud*	1
22	Dati Residenti fuori dall'UE	3
23	Dati trattati attraverso l'utilizzo di device portatili (per es. tablet), anche da parte dei dipendenti	1
24	Permesso l'utilizzo di supporto removibili per il trasferimento dei dati	2

DPIA - Allegato 2 - Criteri di valutazione dell'Impatto

Criteri di valutazione dell'Impatto		
Valutazione	**Scala**	**Descrizione**
MASSIMO	4	Informazioni che, se divulgate, potrebbero avere delle conseguenze quasi irreversibili per l'interessato: elevati problemi finanziari, problemi fisici e psicologici di lungo termine (es. dettagli giudiziari, dati relativi alla salute etc.).
SIGNIFICATIVO	3	Informazioni che, se divulgate, potrebbero avere significative conseguenze per l'interessato: peggioramento stato di salute, perdita del lavoro, rischio di essere inserito in *black list* (es. morosità esattoriale etc.).
LIMITATO	2	Informazioni che, se divulgate, potrebbero causare all'interessato problemi di carattere personale: danno economico, stress, impossibilità di accedere a determinati servizi/prodotti, lieve danno fisico (es. dettagli note spese, CV, retribuzione, benefit sociali).
TRASCURABILE	1	Informazioni quasi pubbliche che, nel caso fossero divulgate a persone non autorizzate, non creerebbero nessuna problematica all'interessato (es. dati pubblici, numero di telefono fisso privato presente negli elenchi telefonici).

DPIA - Allegato 3 - Criteri di valutazione della Probabilità di accadimento

Criteri di valutazione della Probabilità di accadimento		
Valutazione	**Scala**	**Descrizione**
EVENTO PROBABILE	4	Il trattamento avviene con frequenza giornaliera (almeno una volta al giorno).
EVENTO POSSIBILE	3	Il trattamento avviene con frequenza settimanale (almeno una volta a settimana).
EVENTO IMPROBABILE	2	Il trattamento avviene con frequenza mensile/ trimestrale (almeno una volta al mese o a trimestre).
EVENTO RARO	1	Il trattamento avviene con frequenza semestrale/ annuale (almeno una volta a semestre/anno).

DPIA - Allegato 4 - Dettaglio controlli per trattamenti elettronici

#	Dominio ISO/IEC 27001/2013	Obiettivo
1	**Politiche per la sicurezza delle informazioni**	Fornire indicazioni di gestione e supporto per la sicurezza delle informazioni in accordo con i requisiti di *business* e regolamenti cogenti.
2	**Organizzazione della sicurezza delle informazioni**	Stabilire un quadro di gestione per avviare e controllare l'implementazione della sicurezza delle informazioni all'interno dell'organizzazione.
3	**Sicurezza delle risorse umane**	Assicurare che il personale comprenda le proprie responsabilità e sia adeguato al ruolo loro assegnato.
4	**Gestione degli *asset***	Identificare gli *asset* dell'organizzazione e definire appropriate responsabilità per la loro protezione.
5	**Controllo degli accessi**	Prevenire l'accesso di utenti non autorizzati ai sistemi ed alle applicazioni.
6	**Crittografia**	Proteggere la riservatezza, l'autenticità o l'integrità delle informazioni attraverso strumenti di crittografia.
7	**Sicurezza fisica e ambientale**	Prevenire accessi fisici non autorizzati, intromissioni e danni alle infrastrutture informative ed alle informazioni.
8	**Sicurezza delle attività operative**	Assicurare una gestione operativa corretta e sicura delle apparecchiature per l'elaborazione delle informazioni.
9	**Sicurezza delle comunicazioni**	Assicurare la salvaguardia delle informazioni in rete e la protezione dell'infrastruttura di supporto.
10	**Acquisizione, sviluppo e manutenzione dei sistemi informativi**	Assicurare che la sicurezza sia parte integrante dei sistemi informativi in tutto il ciclo di vita. Esso include anche i requisiti per i sistemi informativi che forniscono servizi sulle reti pubbliche.
11	**Relazioni con i fornitori**	Assicurare la protezione degli *asset* dell'organizzazione accessibili ai fornitori.
12	**Gestione degli incidenti relativi alla sicurezza delle informazioni**	Assicurare un approccio efficace e consistente alla gestione degli incidenti di sicurezza informatica, inclusi tutti gli eventi e le vulnerabilità di sicurezza delle comunicazioni.
13	**Disaster Recovery / Business Continuity**	La continuità della sicurezza delle informazioni dovrebbe essere integrata all'interno del sistema di gestione della continuità operativa dell'organizzazione.
14	**Conformità**	Evitare la violazione di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni e di eventuali requisiti di sicurezza.

DPIA - Allegato 5 – Scala di valutazione del livello di Rischio Residuo

		Intervallo Numerico Rischio	
	Livello Rischio Residuo	**Da**	**a**
Trascurabile	Trascurabile	0	2
	Molto - Basso	2	4
Basso	Basso	4	6
	Medio - Basso	6	8
Medio	Medio	8	10
	Medio - Alto	10	12
Alto	Alto	12	14
	Molto - Alto	14	16