MANUALE DELLE PROCEDURE

DEL SISTEMA GESTIONE AZIENDALE PROTEZIONE DATI PERSONALI

	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	**Tullio Zampieri**	Designato di Supporto del SGA PDP		
Validato:	Chiara Zambon	DPO		
Verificato:	Marzia Serafini	COORDINATORE TEAM MULTIDISCIPLINARE del SGA PDP		
Approvato:	Michela Barbiero	Direttore Amministrativo		

Il presente Manuale delle Procedure del SGA PDP - v0 vuole essere il documento di raccolta di linee guida, procedure e istruzioni operative del Sistema Gestione Aziendale Protezione Dati Personali.

Tali documenti potranno essere in futuro integrati e revisionati, secondo principi di accountability ed in ragione di eventuali modifiche normative che ne impongano la revisione e/o modifica.

DOCUMENTI:

-Procedura "Esercizio diritti degli interessati
in materia di protezione dati personali"
allegato 1
allegato 2
allegato 3
allegato 4
allegato 5

-Procedura operativa di gestione notifica violazioni personale (Data Breach)
Allegato 1
Allegato 2

-Procedura di applicazione del principio di Privacy by Design e Privacy by Default
Allegati 1

Linee guida metodologiche per la conduzione del Risk Assessment
e del Data Protection Impact Assessment (DPIA)

Documento di Nomina Autorizzati al trattamento

Documento di Nomina Amministratore di Sistema (ADS).

PROCEDURA TRASVERSALE

GESTIONE E NOTIFICA DI VIOLAZIONE DI DATI PERSONALI (*Data Breach*)

	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	**Tullio Zampieri**	**Designato di Supporto SGA PDP**		
Validato:	Chiara Zambon	DPO		
Verificato:	Marzia Serafini	Coordinatore TEAM MULTIDISCIPLINARE		
Approvato:	Michela Barbiero	Direttore Ammnistrativo		

INDICE

1.PREMESSA

Il presente documento "Gestione e notifica del Data Breach" è stato redatto tenendo in considerazione le indicazioni del Regolamento (UE) 2016/679 e, nello specifico gli articoli 33 e 34, nonché le *Guidelines on Personal Data Breach Notification under Regulation* 2016/679 (wp250rev.01) del WP 29, come previsto dalla Delibera aziendale n. 520 del 22.7.2020.

Successivamente viste *le Guidelines 01/2021 on Examples regarding Personal Data Breach Notification Adopted on 14 December 2021 Version 2.0* e la revisione Sistema Gestione Aziendale Protezione Dati Personali SGA PDP con Delibera n. 323 del 29.4.2022, viene prevista la presente revisione della procedura tenuto conto che sono stati individuati nuovi soggetti/strutture di riferimento:

- **l'Ufficio Protezione Dati Personali** (PDP), incardinato nell'UOC Affari Generali, quale struttura di supporto al Titolare del Trattamento nella gestione del Sistema Gestione Protezione Dati Personali
- **un Referente Protezione Dati Personali** (RPDP) (ex referente privacy aziendale)
- **un Team multidisciplinare** (rappresentativo delle aree aziendali amministrative-gestionali, informatiche sanitarie, territoriali) con funzioni di analisi e supporto all'ufficio PDP, al Referente PDP, al RPD aziendale affinchè siano punti di riferimento, unitamente con il RPD, per l'evoluzione delle disposizioni applicative che saranno necessarie nel tempo.

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*.

In particolare, può trattarsi di "violazione R.I.D.":

- "**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).

2.SCOPO

Scopo del seguente documento è definire attività, ruoli e responsabilità per la gestione e notifica di una violazione di dati personali (Data Breach) in linea con l'evoluzione del sistema normativo e del Sistema Gestione Dati Personali aziendali.

3.CAMPO DI APPLICAZIONE E DESTINATARI

La procedura si applica a tutto il contesto aziendale. I destinatari sono tutti i dipendenti e collaboratori a qualsiasi titolo coinvolti nel trattamento di dati personali.

4.GRUPPO DI LAVORO

Nome e Cognome	Ruolo	Figura professionale	U.O Afferenza
Tullio Zampieri	Coordinatore GdL	Designato di Supporto SGA PDP	Referente SGA PDP
Giulia Gusella	Componente GdL	Collaboratore Prof.le Amm.vo	Ufficio PDP – UOC Affari Generali
Griggio Daniele	Componente GdL	Assistente Amministrativo	Ufficio PDP – UOC Affari Generali
Marco Calore	Componente GdL	Collaboratore Tecnico Prof.le	UOSD Sistemi Informativi
Marzia Serafini	Componente GdL	Coordinatore Team multidisciplinare SGA PDP	UOS Qualità e Percorsi Accreditamento

5.GLOSSARIO E ACRONIMI

Glossario	**Definizione**
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.
Regolamento (UE) 2016/6792016/679	Regolamento Generale sulla protezione dei Dati 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
ACRONIMI	
TT	Titolare del Trattamento
RT	Responsabile del Trattamento
R PDP	Referente Protezione Dati Personali (ex Referente Privacy)
Ufficio PDP	Ufficio Protezione Dati Personali (ex Ufficio Privacy)
SGA PDP	Sistema Gestione Aziendale Protezione Dati Personali
RDP/DPO	Responsabile Protezione Dati / Data Protection Officer

6.DIAGRAMMA DI FLUSSO

RESPONSABILITA'	ATTIVITA'	NOTE
		Vedi punto 7

7.MODALITÀ OPERATIVA

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.

7.1. Rilevazione/Valutazione del *Data Breach*

Ai sensi dell'art. 4 n. 12) del Regolamento (UE) 2016/679 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*.

In particolare, può trattarsi di "violazione R.I.D.":

- "**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;
- 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 dipendente (Designato di supporto, Designato di struttura, Autorizzato al trattamento, Autorizzato di supporto, ecc.), ogni qualvolta rilevi un avvenuto o potenziale *Data Breach*, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del Trattamento, per il tramite del Designato del trattamento competente ovvero il Direttore della struttura di riferimento nonchè inviando tempestivamente una comunicazione all'indirizzo email: privacy@aulss6.veneto.it e al Designato SSI – RSI – STD all'email risultante nell'intranet aziendale.
Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa, ai sensi dell'art. 33 comma 2, Regolamento (UE) 2016/679 il Titolare del trattamento senza ingiustificato ritardo, e comunque entro i termini fissati nel contratto di nomina RT ex art. 28 del GDPR, mediante comunicazione al Designato del trattamento che ha sottoscritto il contratto di nomina RT medesimo, all'email risultante nell'intranet aziendale.
Il Titolare del trattamento, avuta notizia dell'avvenuto o potenziale *Data Breach*, per il tramite del Designato di Supporto avvia l'istruttoria per l'identificazione dell'evento, convoca il GRUPPO DI RISPOSTA (ovvero un gruppo di indagine ristretto composto da soggetti a supporto del Titolare per la gestione dell'evento di violazione, composto dal Designato di Supporto, dal Designato di Struttura coinvolto nel breach, dal Designato SI, dal componente del Team Multidisciplinare rappresentativo dell'area coinvolta, dal Risk Manager).
In questa fase, il Titolare del trattamento ha la possibilità di consultare il DPO per funzioni di indirizzo, anche utilizzando apposita modulistica (*allegato 1*).
Il Titolare del trattamento, per il tramite del Designato di Supporto con l'ausilio dell'Ufficio PDP, procede alla compilazione del Registro Interno delle Violazioni indipendentemente dalle notifiche che saranno effettuate all'Autorità di controllo. Tale registro ha la funzione di documentare tutti i *Data Breach* rilevati e valutati dal Gruppo di Risposta secondo quanto prescritto dalle Linee Guida Enisa 2013.
Il Registro Interno delle Violazioni può avere anche connotazione digitale laddove rientri tra le funzionalità del gestionale relativo al RdT.

7.2. Gestione del Data Breach

Le violazioni che vengono valutate dal Gruppo di Risposta, con **grado di rischio basso per i diritti e le libertà degli interessati,** vengono solamente registrate nel Registro Interno delle Violazioni, correlate da specifica e dettagliata relazione, comprensiva di tutti gli elementi informativi e delle valutazioni in merito effettuate, redatta dal Titolare del Trattamento per il tramite del Designato di Supporto e con l'ausilio dell'Ufficio PDP, sentito anche il DPO. Qualora il Titolare del trattamento ed il DPO (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.

Per le violazioni che vengono valutate dal Gruppo di Risposta con **grado medio-alto per i diritti e le libertà degli interessati**, il titolare del trattamento, per il tramite del Designato di Supporto con l'ausilio del medesimo Gruppo di Risposta e dell'Ufficio PDP procede nella gestione del *Data Breach* avviando un'istruttoria, per raccogliere tutte 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 procedere nella compilazione della modulistica per la notifica al Garante.

A tal fine nella gestione del Data Breach il Gruppo di Risposta dovrà 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*.

Il Gruppo di Risposta, prima di comunicare l'esito dell'istruttoria al Titolare del trattamento, per il tramite del Designato di Supporto, può avvalersi del supporto del RPD nei casi di particolare complessità, per ricevere indicazioni di indirizzo.

7.3. 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 quando sia rilevato grado elevato di rischio per i diritti e le libertà degli interessati (Linee Guida Enisa 2013).

In tal caso il Titolare del trattamento, per il tramite del Designato di Supporto con l'ausilio dell'ufficio PDP, effettua la notifica all'Autorità Garante, con eventuale supporto del Team Multidisciplinare, utilizzando il format (*allegato 2*) e le procedure previste dall'Autorità Garante **entro 72 ore** dal momento in cui ne sia venuto a conoscenza.

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, per il tramite del Designato di Supporto con l'ausilio dell'Ufficio PDP, 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.

7.3.1 Procedura telematica di notifica

Dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ - come indicato dal Provvedimento del 27 maggio 2021.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il GPDP ha ideato e messo disposizione un apposito strumento di autovalutazione (*self assessment)* che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

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.

7.4. 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, per il tramite del Designato di Supporto con l'ausilio dell'Ufficio PDP, ai sensi dell'art. 34 del Regolamento, 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:

1. 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;
2. 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;
3. 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, per il tramite del Designato di Supporto con l'ausilio dell'Ufficio PDP, pone in essere tutte le attività necessarie per ottemperare al provvedimento.

7.5. Pianificazione degli audit

Il RPD procederà, nel corso della propria attività di vigilanza, con cadenza almeno annuale, alla verifica sulla tenuta del Registro interno delle violazioni e delle segnalazioni di violazione dei Data Breach.

7.6. Archiviazione

Il Titolare del trattamento, per il tramite del Designato di Supporto con l'ausilio dell'Ufficio PDP, 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.

8.MATRICE DELLE RESPONSABILITÀ

La tabella propone una sintesi delle attività riconducibili a ciascuna risorsa, sia interna che esterna all'Azienda, coinvolta nel processo di gestione del *Data Breach*.

		Titolare del trattamento		**Responsabile del trattamento** (se coinvolto)	**Responsabile della protezione dei dati (RPD)**
FASE ATTIVITÀ	**Rilevazione/Valutazione**	per il tramite del Designato del Trattamento e con ausilio Ufficio PDP, Designato di Supporto Designato del trattamento SI	RD	RD	FI
	Gestione	per il tramite del Designato di Supporto e con ausilio Ufficio PDP e del GRUPPO DI RISPOSTA	RD	C	FI
	Notifica al Garante (entro 72 ore)	per il tramite del Designato di Supporto e ausilio Ufficio PDP (con supporto eventuale del Team Multidisciplinare)	RD		FI
	Comunicazione agli interessati	per il tramite del Designato di Supporto e con ausilio Ufficio PDP	RD	PC	PC
	Audit interni		PC		RD
	Archivio della documentazione	Ufficio PDP	RD		

Legenda di lettura della tabella
(RD = Responsabilità Diretta del soggetto / PC = Per Conoscenza / C = Collaborazione / FI = Funzioni di indirizzo)

9.ELENCO ATTREZZATURE

Nessuna

10.REQUISITI DI COMPETENZA DEL PERSONALE CHE OPERA NEL PROCESSO

Personale con competenze specifiche legate all'attività di gestione aziendale del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito anche "Regolamento").

11.INDICATORI

(Gli indicatori sono strumenti di monitoraggio e divulgazione delle informazioni. Essi esprimono una determinata caratteristica attraverso un significato sintetico. Sono gli strumenti in grado di misurare l'andamento del fenomeno che si ritiene rappresentativo per l'analisi e sono utilizzati per monitorare e valutare il grado di successo, oppure l'adeguatezza delle attività implementate).

Indicatore di processo:

nr. di violazioni inserite nel Registro Violazioni Interne/anno di riferimento/DPO

nr. di notifiche con procedura telematica al Garante Protezione Dati personali/anno di riferimento/Ufficio PDP

nr. di comunicazioni agli interessati poste in essere/anno di riferimento/Ufficio PDP

12. DIFFUSIONE, CONSERVAZIONE E ARCHIVIAZIONE

La diffusione del presente documento viene effettuata dalla QA/U.O attraverso:

- News aziendale;
- Intranet al link https://intranet.aulss6.veneto.it/pages/docbrowser sezione "Documenti"
- Via mail ai DIR e coordinatori di UUOO

Il documento originale è conservato presso la QA (una copia nella U.O redattrice) e archiviato secondo le indicazioni fornite dal Documento Massimario di scarto aziendale. La QA garantisce l'eliminazione dal sito intranet dei documenti "superati".

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.

13.RIFERIMENTI BIBLIOGRAFICI, NORMATIVI E SITOGRAFIA

La procedura è redatta tenendo in considerazione:

- Regolamento (UE) 2016/6792016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito Regolamento) e, nello specifico, gli articoli 33 e 34;

- le Guidelines on Personal Data Breach Notification under Regulation 2016/679 (wp250rev.01) del WP29;
- Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013 - Enisa

14.TEMPI DI ENTRATA IN VIGORE

La Procedura operativa è entrata in vigore il

15. ALLEGATI

Allegato 1: Modulo di richiesta consulenza al RPD

Allegato 2: Format come da procedura telematica del Garante Protezione Dati Personali per la notifica del Data Breach sul portale dell'Autorità

REGIONE DEL VENETO
ULSS6 EUGANEA

Regione del Veneto
AZIENDA U.L.S.S. N. 6 EUGANEA
www.aulss6.veneto.it – P.E.C.: protocollo.aulss6@pecveneto.it
Via Enrico degli Scrovegni n. 14 – 35131 PADOVA

Cod. Fisc. / P. IVA 00349050286

UOC ……

Prot. n. Padova ……..

Al Responsabile della Protezione dei Dati
AULSS 6 EUGANEA
E-mail: _____

Oggetto: Richiesta consulenza al RPD per Data Breach

Il sottoscritto …….. in qualità di …….. dell'Azienda ULSS 6 Euganea 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

Allegato 1 alla procedura per il Data Breach

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

V.2021-04

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …….. Nome[1*] …….
E-mail[2*] ……
nella sua qualità[3] di

0 rappresentante legale

0 delegato del rappresentante legale

Cognome[4*] …….. Nome[4*] …….

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

———————————

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

0 ***Prima notifica***

0 a) Completa

0 b) Preliminare[1]

La notifica viene effettuata

0 ai sensi dell'art. 33 del RGPD

0 ai sensi dell'art. 26 d.lgs. 51/2018

0 ***Notifica integrativa***[2]

0 c) fascicolo n. [3*] ..... PIN [3*] .....

———————————

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per completare il processo di notifica.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- 0 a) Fornire ulteriori informazioni senza completare il processo di notifica
- 0 b) Fornire ulteriori informazioni e completare il processo di notifica
- 0 c) Completare il processo di notifica senza fornire ulteriori informazioni
- 0 d) Annullare una precedente notifica per le seguenti motivazioni:

C) Titolare del trattamento

1. *Il titolare del trattamento è:*

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

0 Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

0 Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
(*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)

0 Non censito in nessuno dei due precedenti indici

2. *Dati del titolare del trattamento*

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* .....
Codice Fiscale [1]* ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato* .....
Provincia* ..... Comune* ..... CAP* .....
Indirizzo* .....
Telefono* .....
E-mail[2]* .....
PEC[2]* .....

———————————

[1] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

0 a) Compila la sezione

0 b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] .....

Codice Fiscale/P.IVA* ..... Soggetto privo di C.F./P.IVA italiana ☐

Stato* .....

Provincia* ..... Comune* ..... CAP* .....

Indirizzo* .....

Telefono* .....

E-mail[2*] .....

PEC[2*] .....

———————————

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni (cfr. art. 33, par. 3, lett. b), del Regolamento).

o ***1) Responsabile della protezione dei dati***

- o i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1*] n.……..
- o i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……

o ***2) Altro soggetto***

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……
Funzione rivestita* ……

———————————

[1] Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto che sarà comunicato con una successiva notifica integrativa.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

———————————

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

  Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- o a) Il ___ /___ /_____
- o b) Dal ___/___ /_____ (la violazione è ancora in corso)
- o c) Dal ___/___ /_____ al ___ /___ /_____
- o d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- o a) Rilevazione da parte del titolare[1]
- o b) Comunicazione da parte del responsabile del trattamento
- o c) Segnalazione da parte di un interessato
- o d) Segnalazione da parte di un soggetto esterno
- o e) Notizie stampa
- o f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …… **Ora** ……..

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

o a) N. …….. interessati
o b) Circa n. …….. interessati
o c) Non determinabile
o d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. *Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione*

o a) N. ……..
o b) Circa n. ……..
o c) Non determinabile
o d) Non ancora determinato

14. *Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati*

15. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
[ ] d) Altro

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

o a) Trascurabile
o b) Bassa
o c) Media
o d) Alta
o e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future

3. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- o a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il ___/___/_____
- o b) No, sarà comunicata entro il ___/___/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare 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 (es. cifratura);

Descrivere le misure applicate

[ ] e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

2. Numero di interessati a cui è stata comunicata la violazione

N. …….. interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica
[ ] d) Altro

4. Contenuto della comunicazione agli interessati

5. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?

O Sì O No

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O Sì O No

Note

———————————

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. ***La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?***

   - o a) Sì
   - o b) No
   - o c) Sono tuttora in corso le dovute valutazioni

2. ***Indicare l'autorità di controllo capofila[1]***

   - o a) Garante per la protezione dei dati personali
   - o b) Altra autorità di controllo: [Selezionare]
   - o c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. ***Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione***

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

———————————

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   o a) Sì
   o b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

   [ ] Austria
   [ ] Belgio
   [ ] Bulgaria
   [ ] Cipro
   [ ] Croazia
   [ ] Danimarca
   [ ] Estonia
   [ ] Finlandia
   [ ] Francia
   [ ] Germania
   [ ] Grecia
   [ ] Irlanda
   [ ] Islanda
   [ ] Lettonia
   [ ] Liechtenstein
   [ ] Lituania
   [ ] Lussemburgo
   [ ] Malta
   [ ] Norvegia
   [ ] Paesi Bassi
   [ ] Polonia
   [ ] Portogallo
   [ ] Rep. Ceca
   [ ] Romania
   [ ] Slovacchia
   [ ] Slovenia
   [ ] Spagna

[ ] Svezia
[ ] Ungheria

3. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

PROCEDURA TRASVERSALE

ESERCIZIO DIRITTI DEGLI INTERESSATI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

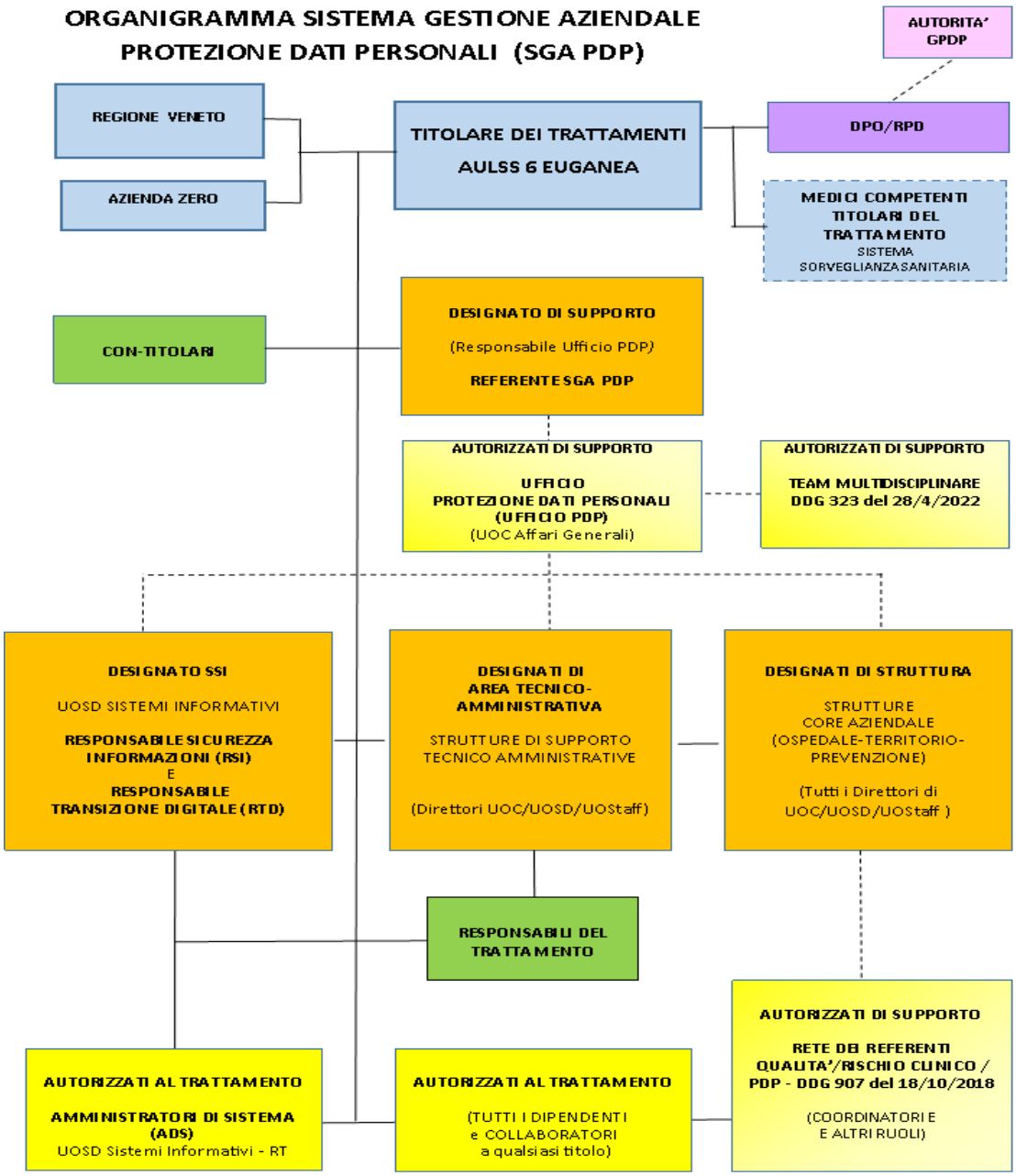
	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	Tullio Zampieri	Designato di Supporto del SGA PDP		
Validato:	Chiara Zambon	DPO		
Verificato:	Marzia Serafini	COORDINATORE TEAM MULTIDISCIPLINARE del SGA PDP		
Approvato:	Barbiero Michela	Direttore Amministrativo		

INDICE

1. PREMESSA

La presente procedura operativa "Esercizio diritti degli interessati in materia di protezione dati personali" è stata redatta tenendo in considerazione le indicazioni del Regolamento (UE) 2016/679 e, nello gli articoli 15, 16, 17, 18, 20, 21, 22 e 77 del Regolamento (UE) 2016/679 e, come previsto dalla Delibera aziendale n. 520 del 22.7.2020

Successivamente viste le modifiche apportate al Sistema Gestione Aziendale Protezione Dati Personali SGA PDP e individuate i soggetti di riferimento per la messa in opera dello stesso:



2.SCOPO

Scopo del seguente documento è definire le modalità di gestione delle istanze per l'esercizio dei seguenti diritti degli interessati per i trattamenti di dati personali da parte dell'Azienda ULSS 6 Euganea:

- diritto di accesso ai dati,
- diritto di rettifica,
- diritto di cancellazione, ove consentito dalle normative vigenti,
- diritto di limitazione di Trattamento;
- diritto alla portabilità, nei limiti disposti dall'art.20 Gdpr e limitatamente ai dati amministrativo/contabili e ai dati per i quali non vi sono disposti normativi specifici per la loro acquisizione;
- diritto di opposizione;
- diritto di non essere sottoposto a decisioni basate unicamente su trattamenti automatizzati;
- diritto di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento;
- diritto di reclamo all'Autorità Garante per la Protezione dei Dati Personali.

3.CAMPO DI APPLICAZIONE E DESTINATARI

Il seguente documento si applica ai trattamenti di dati personali di cui l'Azienda è titolare, viene attuata in caso di richiesta di esercizio dei diritti da parte degli interessati (utenti, assistiti, familiari degli assistiti o soggetti che ne hanno la tutela, dipendenti, collaboratori a qualsiasi titolo, fornitori di beni e servizi, ecc.)
La procedura è emanata a cura dell'Azienda ULSS 6 Euganea ed è destinata a tutti agli operatori dell'Ufficio PDP, al Designato di Supporto, ai Designati di Struttura, agli Autorizzati al Trattamento, agli Autorizzati di supporto (Team Multidisciplinare, Rete dei Referenti).

4.GRUPPO DI LAVORO

Nome e Cognome	Ruolo	Figura professionale	U.O Afferenza
Tullio Zampieri	Coordinatore GdL	Direttore	UOC Affari Generali
Giulia Gusella	Componente GdL	Assistente amministrativo	UOC Affari General
Chiara Zambon	Componente GdL	Data Protection Officer	UOC Affari Generali
Marzia Serafini	Componente GdL	Referente Qualità	UOS Qualità e Percorsi di Accreditamento

5.GLOSSARIO E ACRONIMI

Glossario	Definizione
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.
Designato di Supporto	Referente del SGA PDP – Responsabile Ufficio Protezione Dati Personali
Designato di Struttura	Direttore/Responsabile di UOC/UOSD/UOS di Staff del SGA PDP
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 GDPR)	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 GDPR)**	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 **(CD "diritto all'oblio")** **(Art. 17 del GDPR)**	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

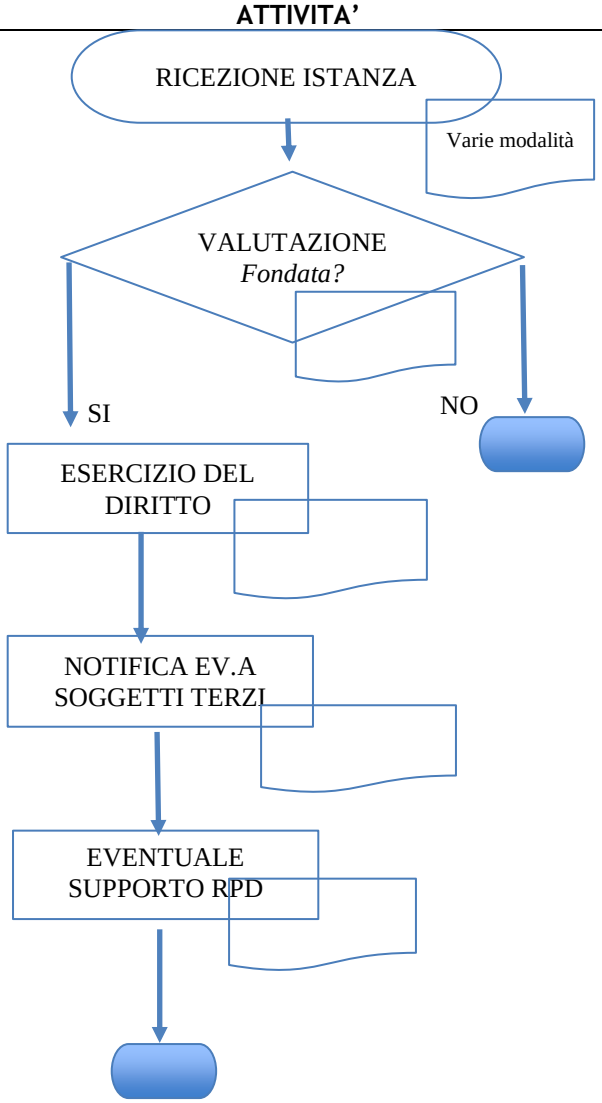
	il Trattamento; c) l'interessato si oppone al Trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al Trattamento, oppure si oppone al Trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; 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 GDPR)	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 GDPR)	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 GDPR)	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 GDPR)	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.
Diritto di reclamo al GPDP (art. 77 del GDPR)	1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il Trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. 2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.
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.
Acronimi	
GPDP	Autorità Garante per la Protezione dei Dati Personali
GDPR	Regolamento (UE) 2016/679
UPDP	Ufficio Protezione Dati Personali
SGA PDP	Sistema Gestione Aziendale Protezione Dati Personali

RdT	Registro delle Attività di Trattamento
RPD/DPO	Responsabile Protezione Dati / Data Protection Officer

6. DIAGRAMMA DI FLUSSO

RESPONSABILITA'	ATTIVITA'	NOTE
		Vedi punto 7.1-7.1.1-7.1.2 Allegato 1, 2 e 3 Vedi punto 7.2 Allegato 3, 4 e 5 Vedi punto 7.3-7.3.1-7.3.2 Allegato 6 Vedi punto 7.4 Vedi punto 7.5

7. MODALITÀ OPERATIVA

Il processo di gestione delle istanze degli interessati, ovvero tutti i soggetti i cui dati personali vengono trattati nell'espletamento delle attività poste in essere dall'Azienda (utenti, assistiti, pazienti, familiari e soggetti che detengono la responsabilità genitoriale, dipendenti, collaboratori a vario titolo, fornitori di beni

e servizi, ecc.), per esercitare i loro diritti sui trattamenti di dati personali, posti in essere dal Titolare del Trattamento (Azienda ULSS 6 Euganea), si espleta mediante le seguenti fasi:

7.1 Ricezione dell'istanza

7.1.1 Ricezione dell'istanza da parte dell'Ufficio Protezione Dati Personali e/o del RPD

7.1.2 Ricezione dell'istanza da parte del Responsabile del Trattamento

7.2 Valutazione dell'istanza;

7.3 Esercizio del diritto;

7.3.1 Risposta all'interessato;

7.3.2. Archivio della documentazione

7.4 Notifica della richiesta a soggetti terzi;

7.5. Eventuale parere al RPD

Le informazioni generali e quelle più specifiche sul Trattamento dei dati personali, nell'ambito delle attività trattamentali dell'Azienda, come previsto dagli artt. 13 e 14 del GDP, fornite agli interessati, riportano i dati di contatto per l'inoltro dell'istanza di esercizio dei diritti. Nello specifico, gli interessati possono inviare una comunicazione secondo quanto indicato al punto 7.1.

7.1. Ricezione dell'istanza

La richiesta di esercizio dei diritti da parte degli interessati deve essere presentata con le seguenti modalità ovvero l'invio di:

- una semplice richiesta scritta, da inviare alla sede legale (Via Scrovegni, 14 Padova, Ufficio PdP) del Titolare del Trattamento, all'attenzione del RPD e/o dell'ufficio Protezione Dati Personali;
- una richiesta su modulo predisposto, pubblicato sul sito web aziendale (www.aulss6.veneto.it), alla sezione "Sistema Privacy Aziendale" – Esercizio dei Diritti all'indirizzo e-mail: privacy@aulss6.veneto.it (*Allegato 1*);
- una semplice richiesta e-mail all'indirizzo del RPD (rpd@aulss6.veneto.it).

Quando perviene una tal richiesta al Titolare del Trattamento, questi, con l'ausilio dell'Ufficio PDP, prende in carico l'istanza del cittadino, comunica la richiesta ricevuta al Designato di Supporto e attiva, **entro cinque giorni** dalla ricezione il Designato di Struttura che ne abbia la competenza in relazione all'oggetto dell'istanza.

Il Designato di Supporto, è tenuto in collaborazione con l'ufficio PDP, a registrare la richiesta ricevuta nel Registro delle Istanze degli Interessati *(Allegato 2)*.

Tale registro può avere anche connotazione digitale laddove rientri tra le funzionalità del gestionale relativo al Registro delle Attività di Trattamento (RdT).

7.1.1 Ricezione dell'istanza da parte del RPD/DPO

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 Designato di Supporto tramite e-mail affinché il medesimo provveda, con l'ausilio dell'ufficio PDP, all'espletamento della procedura di cui al 7.1. In tale caso il RPD sarà tenuto informato, per conoscenza, del processo di evasione della richiesta verso l'Interessato. Il RPD, in ogni caso, ha facoltà di effettuare controlli dell'avvenuta evasione della richiesta, monitorandone la procedura.

7.1.2 Ricezione dell'istanza da parte del Responsabile del Trattamento

Qualora il Responsabile del Trattamento ricevesse la richiesta di esercizio di diritti dall'interessato provvederà all'inoltro della richiesta al Titolare del Trattamento ai contatti indicati nei contratti di nomina ex art. 28 del GDPR.

Tale richiesta sarà di seguito inoltrata al Designato di Supporto, (tramite e-mail) affinché il medesimo provveda, con l'ausilio dell'ufficio PDP, all'espletamento della procedura di cui al 7.1.

Il Responsabile del Trattamento sarà tenuto informato, per conoscenza, del processo di evasione della richiesta verso l'Interessato.

7.2. Valutazione dell'istanza

Il Designato di Supporto, con l'ausilio dell'Ufficio PDP, in collaborazione del Designato di Struttura che ha effettuato il Trattamento di dati personali cui si riferisce l'istanza dell'interessato, ed eventualmente con il supporto del Designato SSI – RSI - STD (Direttore UOSD Sistemi Informativi) e, qualora necessario, del Responsabile del Trattamento coinvolto nel processo, 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 7.1 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 informatici o presso archivi analogici, ecc…).

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

Il Titolare del Trattamento, per il tramite del Designato di supporto, valuterà 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 interromperà i termini di risposta comunicando al soggetto l'estensione dei termini a ulteriori 60 giorni come indicato al successivo punto sull'esercizio del diritto *(allegato 5)*.

7.3. Esercizio del diritto

Il Titolare del Trattamento, per il tramite del Designato di supporto, con l'ausilio dell'Ufficio PDP, con la collaborazione del Designato di Struttura che ha effettuato il Trattamento di dati personali cui si riferisce l'istanza dell'interessato, ed eventualmente il supporto del Designato SSI – RSI - STD (Direttore UOSD Sistemi Informativi) e, qualora necessario, del Responsabile del Trattamento, provvede ad ottemperare a quanto richiesto dall'interessato nell'esercizio degli specifici diritti:

- diritto di accesso ai dati
- diritto di rettifica,
- diritto di cancellazione e Diritto all'Oblio, ove consentiti dalle normative vigenti,
- diritto di limitazione di trattamento,
- diritto alla portabilità nei limiti disposti dall'art.20 GDPR e limitatamente ai dati amministrativo/contabili e ai dati per i quali non vi sono disposti normativi specifici per la loro acquisizione (p.es. copia di cartelle cliniche),
- diritto di opposizione,
- diritto di non essere sottoposto a decisioni basate unicamente su trattamenti automatizzati,
- diritto di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento,
- diritto di reclamo all'Autorità Garante per la Protezione dei Dati Personali.

Laddove il trattamento sia espletato con modalità digitali, il Designato SI indicherà all'UOSD Sistemi Informativi le specifiche procedure idonee all'attuazione delle richieste dell'interessato, in merito ad ogni specifico esercizio di diritti.

7.3.1 Risposta all'interessato

Il Titolare del Trattamento, per il tramite del Designato di Supporto, con l'ausilio dell'ufficio PDP (sentito il parere del RPD ove ritenuto necessario) ai sensi dell'art. 12 del Regolamento fornisce risposta all'interessato *(allegato 6*) 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 Designato di supporto, con l'ausilio dell'ufficio UPDP è tenuto a comunicare la proroga e a fornire riscontro all'interessato in relazione ai motivi della dilazione delle tempistiche.

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 inviare la richiesta 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.

La risposta viene comunicata per conoscenza, con email separate, anche ai seguenti soggetti ove coinvolti come ai punti che precedono (Designato al Trattamento, Designato SSI – RSI - STD) e al Responsabile del Trattamento che abbia ricevuto l'istanza.

7.3.2. Archivio della documentazione

L'ufficio PDP 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. Una volta fornito un riscontro all'interessato richiedente, viene archiviata una copia della comunicazione di risposta, nonché tutta la documentazione pertinente.

7.4. Notifica della richiesta a soggetti terzi

Ai sensi dell'art. 19 del GDPR, il titolare del trattamento, per il tramite del Designato di Supporto, con l'ausilio dell'ufficio PDP, 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, entro il termine di 15 giorni (quindici) 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.

7.5 Eventuale parere al RPD

Laddove necessario, in casi di particolari difficoltà e/o gravità, il Designato di Supporto, con l'ausilio dell'ufficio PDP, può interpellare il RPD/DPO affinché esprima un parere sulla questione.

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

8. MATRICE DELLE RESPONSABILITÀ

		Titolare del Trattamento		Responsabile del Trattamento (se coinvolto)	Responsabile della protezione dei dati (RPD)
FASE ATTIVITÀ	Ricezione dell'istanza	Designato di Supporto Con ausilio di Ufficio PDP	RD	RD	Se riceve direttamente inoltra al Designato di Supporto che ha RD
	Valutazione dell'istanza	Designato di Supporto Con ausilio di Ufficio PDP	RD	C	
		Designato del Trattamento della struttura coinvolta	C		
	Esercizio del diritto;	Designato di Supporto Con ausilio di Ufficio PDP	RD	C	
		Designato del Trattamento della struttura coinvolta	C		
		Designato SI	C		
	Risposta all'interessato;	Designato di Supporto Con ausilio di Ufficio PDP	RD	PC	Eventualmente PC (se aveva ricevuto l'istanza)
	Archivio della documentazione	Ufficio PDP	RD		
	Notifica della richiesta a soggetti terzi;	Designato di Supporto Con ausilio di Ufficio PDP	RD		
	Eventuale parere al RPD	Designato di Supporto Con ausilio di Ufficio PDP	RD		RD

Legenda di lettura (RD = responsabile diretto / PC = per conoscenza / C= collaborazione)

9.ELENCO ATTREZZATURE

Utilizzo dell'applicativo per il Registro dei Trattamenti al fine di tracciare e gestire tutte le richieste di esercizio dei diritti da parte degli interessati

10.REQUISITI DI COMPETENZA DEL PERSONALE CHE OPERA NEL PROCESSO

Personale con competenze specifiche legate all'attività di gestione aziendale del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 di cui al SGA PDP (Autorizzati al trattamento dell'Ufficio Protezione Dati Personali)

11. TRATTAMENTO E MISURE DI PROTEZIONE DEL DATO PERSONALE

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").

12. DIFFUSIONE, CONSERVAZIONE E ARCHIVIAZIONE

La diffusione del presente documento viene effettuata dalla QA/U.O attraverso:

- News aziendale;
- Intranet al link https://intranet.aulss6.veneto.it/pages/docbrowser sezione "Documenti"
- Via mail ai DIR e coordinatori di UUOO
- Pubblicazione sul sito web di Aulss6 in quanto allegato alla delibera di "Riorganizzazione poteri privacy"

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. Il documento originale è conservato presso la U.O redattrice e archiviato secondo le indicazioni fornite dal Documento Massimario di scarto aziendale. La QA garantisce l'eliminazione dal sito intranet dei documenti "superati".

13.INDICATORI

N. istanze ricevute/anno di riferimento/Ufficio PDP

N. pareri RPD/anno di riferimento/RPD

14. RIFERIMENTI BIBLIOGRAFICI, NORMATIVI E SITOGRAFIA

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").

15. TEMPI DI ENTRATA IN VIGORE

L'istruzione operativa entrerà in vigore dal mese di Novembre 2022

16. ALLEGATI

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

All'Azienda ULSS 6 Euganea
Via E. degli Scrovegni, 14
35121 PADOVA

privacy@aulss6.veneto.it

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) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati colti o altrimenti trattati
  b) l'interessato revoca il consenso sui cui si basa il trattamento conformemente all'art. 6, paragrafo 1, lettera a) o all'art. 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'art. 21, paragrafo 1) e non sussiste alcun motivo legittimo prevalente per procedere al trattamento oppure si oppone al trattamento ai sensi dell'art. 21, paragrafo 2);
  d) i dati personali sono stati trattati illecitamente;
  e) i dati personali devono essere cancellati per adempiere ad 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'art. 8, paragrafo 1.

☐ 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):

_____
_____
_____
_____
_____
_____
_____
_____

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):

_____
_____
_____
_____
_____

[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.

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 interessati

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									

Al Responsabile della Protezione Dati
AULSS 6 EUGANEA
Via E. degli Scrovegni
35131 PADOVA
E-mail: rpd@aulss6.veneto.it

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

_____

REGIONE DEL VENETO
ULSS6 EUGANEA

Regione del Veneto
AZIENDA U.L.S.S. N. 6 EUGANEA
www.aulss6.veneto.it – P.E.C.: protocollo.aulss6@pecveneto.it
Via Enrico degli Scrovegni n. 14 – 35131 PADOVA

Cod. Fisc. / P. IVA 00349050286

UOC Affari Generali

Prot. n. Padova

Egr. Sig
_____
_____
_____

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

Con 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.

Distinti saluti

Il Direttore
Dr. Tullio Zampieri

REGIONE DEL VENETO
ULSS6 EUGANEA

Regione del Veneto
AZIENDA U.L.S.S. N. 6 EUGANEA
www.aulss6.veneto.it – P.E.C.: protocollo.aulss6@pecveneto.it
Via Enrico degli Scrovegni n. 14 – 35131 PADOVA

Cod. Fisc. / P. IVA 00349050286

UOC Affari Generali

Prot. n. Padova

Egr. Sig
_____
_____
_____

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

Con 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:
……
……
……
……
……

Distinti saluti

Il Direttore
Dr. Tullio Zampieri

REGIONE DEL VENETO
ULSS6 EUGANEA

Regione del Veneto
AZIENDA U.L.S.S. N. 6 EUGANEA
www.aulss6.veneto.it – P.E.C.: protocollo.aulss6@pecveneto.it
Via Enrico degli Scrovegni n. 14 – 35131 PADOVA

Cod. Fisc. / P. IVA 00349050286

UOC Affari Generali

Prot. n. Padova

Egr. sig
_____
_____
_____

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

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:
……

Responsabile del procedimento
Referente Privacy Aziendale: Dr. Tullio Zampieri
Tel. 049 8214746 – e-mail: privacy@aulss6.veneto.it

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:
……
……
……..

<u>Diritto alla portabilità</u> (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

Responsabile del procedimento
Referente Privacy Aziendale: Dr. Tullio Zampieri
Tel. 049 8214746 – e-mail: privacy@aulss6.veneto.it

□ 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

Distinti saluti

Il Direttore
Dr. Tullio Zampieri

Procedura Trasversale Guida metodologica per la conduzione del Risk Assessment e del Data Protection Impact Assessment (DPIA)

	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	Tullio Zampieri	Designato di Supporto del SGA PDP		
Validato:	Chiara Zambon	DPO		
Verificato:	Marzia Serafini	COORDINATORE TEAM MULTIDISCIPLINARE del SGA PDP		
Approvato:	Barbiero Michela	Direttore Amministrativo		

INDICE

1. Introduzione e obiettivi del documento

o 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 **"*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.

o 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 6 Euganea, 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**.

2. 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.

[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."

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

3. 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]
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*"

E' 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

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

nella migliore conformazione al GDPR e soprattutto nella migliore dimostrazione dell'accountability, ossia della capacità di dimostrazione di tale conformazione.

4. 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 del trattamento svolgerà la valutazione d'impatto sulla protezione dei dati che serve ad identificare la necessità di effettuazione di una DPIA seguendo i criteri che precedono, in collaborazione con l'Ufficio PDP peri nuovi trattamenti di dati personali e per quelli già svolti cui sono apportate modifiche sostanziali. Ha facoltà di consultazione del DPO.

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 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 del trattamento 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).

[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.

5. 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*.

5.1. 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'AULSS 6 Euganea e tracciati all'interno del **"Registro delle 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".

5.2. 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.

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;

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

- 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.

6. 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*.

6.1. 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]

6.2. 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;

[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

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

6.3. 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.

6.4. 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).

6.5. 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.

7. 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.

8. Allegati

- **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 AULSS 6 Euganea o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Cloud / SaaS)	2
20	Infrastruttura (di AULSS 6 Euganea 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

- **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).

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).

-
- **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.

- **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

9. DPIA con software dedicato

L'Azienda ULSS 6 Euganea ha acquisito nel 2019 un applicativo "DATA PROTECTION MANAGEMENT (DPM) per la gestione del registro delle attività di trattamento che consente oltre alla individuazione e mappatura dei trattamenti di dati personali nei processi aziendali anche di porre in essere un sistema di work flow autorizzativo informatico per la profilazione degli utenti interni (abilitazione, disabilitazione, accesso dei

delegati / autorizzati) collegato al sistema gestione risorse umane, per la tracciabilità delle profilazioni degli utenti esterni (Responsabili del trattamento, convenzionati, strutture accreditate, ecc…) nonché alla relativa predisposizione documentale in materiale di privacy.
Lo strumento risulta predisposto anche per espletare la procedura **di valutazione d'impatto** correlata agli elementi acquisiti dal registro dei trattamenti stesso, secondo le linee guida metodologiche sopra descritte, validate dall'Ente di Governance.

Procedura Trasversale

Guida per l'applicazione del principio di Privacy by Design e Privacy by Default

	Nome Cognome	Ruolo/Unità Operativa	Data	Firma
Redatto:	Tullio Zampieri	Designato di Supporto del SGA PDP		
Validato:	Chiara Zambon	DPO		
Verificato:	Marzia Serafini	COORDINATORE TEAM MULTIDISCIPLINARE del SGA PDP		
Approvato:	Barbiero Michela	Direttore Amministrativo		

INDICE

1. 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.**

1.1. 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.

2. 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.

3. Destinatari

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

4. Ruoli e responsabilità

La tabella propone una sintesi delle attività e relative responsabilità riconducibili a ciascuna risorsa, sia interna che esterna all'Azienda, al fine di garantire la corretta applicazione dei principi di *Privacy by Design e Privacy by Default*, ossia di protezione dei dati fin dalla progettazione e protezione degli stessi per impostazione predefinita.

Legenda di lettura della tabella (RD = Responsabilità Diretta / PC = Per Conoscenza / C = Collaborazione

		Titolare del trattamento		Responsabile del trattamento (se coinvolto)	Responsabile della protezione dei dati
FASE ATTIVITÀ	**Mappatura preliminare dei trattamenti**	Il Designato di Struttura	RD		
		Designato SI	C		
		Designato di Supporto e Ufficio PDP	Eventuale supporto		
	Verifica dell'applicabilità dei principi di *privacy* by D&D	Designato di Struttura	RD	C	PC
		Designato SI	C		
	Applicazione dei principi di *privacy* by D&D	Designato di Struttura	RD	C	PC
		UOSD Sistemi Informativi	C		
	Modifica o introduzione di un trattamento	Designato di Struttura	RD	C	PC
	Archivio della documentazione	Designato di Struttura	RD		

5. 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

5.1. Mappatura preliminare

7.1 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

7.2 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.

7.3 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.

In questa fase il Titolare del trattamento (Delegato del trattamento) ha la collaborazione dell'UOS Sistemi Informativi e ove necessario l'eventuale supporto dell'Unità Funzionale Privacy

5.2. 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; può collaborare al riguardo l'UOS Sistemi Informativi.

5.3. 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, per il tramite del Designato di Struttura, 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.

Può collaborare con il Designato di Struttura il Designato SI.

5.4. 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, per il tramite del Designato di Struttura, 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.

5.5. Archiviazione della documentazione

Il Titolare del trattamento, per il tramite del Designato di Struttura, archivia la documentazione e la relazione contenente gli esiti della valutazione finale.

6. Modifiche al presente documento

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

7. Allegati

- Checklist di sicurezza
- Checklist di privacy by design

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

Egregio dipendente/collaboratore,

Premesso che:

- fra Lei e l'Azienda ULSS 6 Euganea (di seguito anche l'Azienda), con sede legale in via Scrovegni, 14 Padova (PD), è in corso un rapporto di lavoro;
- nell'esecuzione delle prestazioni lavorative concordate mediante il contratto di lavoro, Lei può svolgere operazioni di trattamento in relazione ai dati personali di cui l'Azienda è Titolare del trattamento ovvero in relazione ai dati personali che l'Azienda è autorizzata a trattare in qualità di Responsabile o Sub-Responsabile del trattamento;
- Il presente atto di nomina è elaborato nel rispetto della normativa in materia di trattamento dei dati personali come contenuta nel Regolamento UE 2016/679 (di seguito Regolamento UE), nonché nel Codice della Privacy (D.Lgs 196/03) come novellato dal D.Lgs. 101/18.
  Fermo restando che la normativa vigente non pone alcun vincolo di forma in merito alle modalità con cui impartire le istruzioni ai soggetti autorizzati al trattamento dei dati personali, sia l'art. 2 *quaterdecies* del Codice della privacy che l'art. 29 del Regolamento UE richiedono che l'Azienda provveda a fornire apposite istruzioni in materia di trattamento dei dati personali nei confronti di chiunque abbia accesso, sotto la propria autorità, ai dati medesimi;
- Per **dato personale** si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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*".
- Per **trattamento dei dati personali** s'intende il compimento di "*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*".
- Per **Titolare del trattamento** s'intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*".
- Per **Responsabile del trattamento** s'intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento*". Il Responsabile del trattamento può avvalersi di un altro Responsabile del trattamento (c.d. Sub-Responsabile del trattamento), esclusivamente previa autorizzazione del Titolare del trattamento. In capo al Sub-Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto nazionale o dell'Unione, gli stessi obblighi del Responsabile del trattamento.
- L'Azienda precisa che le proprie procedure aziendali, cui Lei dovrà attenersi nell'esecuzione delle Sue mansioni lavorative, sono elaborate nel pieno rispetto dei diritti e delle libertà fondamentali e della normativa in materia di trattamento dei dati personali e sono strutturate al fine di garantire la liceità e correttezza delle operazioni di trattamento sui dati personali;
- **La presente nomina ha l'esclusiva funzione di autorizzarLa al trattamento dei dati personali e di impartirLe le istruzioni di base necessarie al compimento delle operazioni di trattamento sui dati personali, che saranno completate con altre approfondite nelle sessioni formative dedicate**. Si precisa,

inoltre, che la presente nomina non implica né il diritto a percepire uno specifico compenso, indennità o rimborso per l'attività di trattamento dei dati personali, né comporta l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate in virtù del rapporto di lavoro in essere con l'Azienda.

Con la presente, l'Azienda, al fine di garantire la corretta gestione dei dati personali, La autorizza al trattamento dei dati personali contenuti negli archivi cartacei o nelle banche dati elettroniche della Azienda medesima a cui Lei ha accesso, sulla base delle autorizzazioni e abilitazioni all'accesso ai sistemi informativi ed agli archivi cartacei contenute nel Registro dei Trattamenti generate all'inizio della prestazione lavorativa. L'Azienda La invita ad attenersi, scrupolosamente, alle istruzioni di base individuate nella presente nomina, nonché alle successive ed eventuali istruzioni che l'Azienda potrà impartirLe in materia di protezione dei dati personali anche attraverso specifiche sessioni formative.

1. DATI PERSONALI OGGETTO DELLE OPERAZIONI DI TRATTAMENTO

Il trattamento dei dati personali, sia esso in formato elettronico che manuale, potrà realizzarsi nei limiti delle mansioni a Lei affidate in considerazione del rapporto di lavoro in corso con la Azienda.
Le operazioni di trattamento dei dati personali potranno riguardare esclusivamente le seguenti categorie di dati personali contenuti negli archivi cartacei o nelle banche dati elettroniche della Azienda e a cui Lei può accedere:

- **dati personali identificativi riferibili al personale dell'Azienda** (sia esso dipendente o autonomo ex art. 2222 c.c.), dei Clienti o potenziali Clienti, dei Fornitori dell'Azienda o ad altri soggetti terzi con cui l'Azienda intrattiene rapporti nell'ambito della propria attività, soggetti familiari di pazienti e assistiti ovvero soggetti che espletano funzioni di responsabilità genitoriale (amministratori di sostegno, tutori, etc.);
- **dati personali appartenenti alla categoria definita dall'art. 9 Regolamento UE come "particolari",** (tra questi i DATI RELATIVI ALLA SALUTE) riferiti a dipendenti, pazienti ad assistiti dell'Azienda e terzi;
- **dati personali appartenenti alla categoria definita dall'art. 10 Regolamento UE** riferiti a dipendenti, pazienti ad assistiti dell'Azienda e terzi nei limiti da questo previsti (il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati).

Il trattamento di **dati personali appartenenti alle categorie definite dagli artt. 9 e 10 del Regolamento UE** è autorizzato dalla Azienda esclusivamente per espletare gli obblighi normativi applicabili ove il trattamento medesimo sia necessario in considerazione della specifica funzione aziendale a Lei assegnata mediante il contratto di lavoro. In particolare, nel compimento delle operazioni di trattamento su queste ultime categorie di dati personali, Lei è tenuto ad operare con la massima diligenza, correttezza e buona fede imposta in virtù della natura particolarmente "sensibile" dei dati medesimi e comunque riducendo al minimo l'utilizzo di dati personali medesimi.

2. ISTRUZIONI PER IL COMPIMENTO DELLE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI

In qualità di soggetto autorizzato al trattamento dei dati personali, Lei s'impegna a:

a. Trattare i dati personali nel **rispetto del presente atto e comunque nei limiti di quanto necessario e funzionale allo svolgimento delle Sue mansioni**.
b. Trattare i dati personali nel **rispetto della normativa** in materia di trattamento dei dati personali e compiere le operazioni di trattamento in modo lecito, corretto e secondo trasparenza, provvedendo, se

necessario, alla correzione ed aggiornamento dei dati medesimi sulla base delle istruzioni impartite, caso per caso, dalla Azienda. Lei può trattare i dati personali esclusivamente nel **rispetto delle finalità** definite dalla Azienda e, ove ritenga che i dati personali siano eccedenti ovvero non pertinenti o non completi rispetto alle finalità del trattamento, Lei provvede a comunicarlo all'Azienda stessa, per il tramite del Designato di Struttura e il Referente di Rete Protezione Dati Personali. Si precisa, altresì, che la conservazione dei dati medesimi deve limitarsi al periodo di tempo, necessario al raggiungimento delle finalità per cui i dati personali sono trattati, indicato nel Massimario di scarto della ULSS n. 6 Euganea in vigore e che le operazioni di trattamento vanno compiute riducendo al minimo l'utilizzo di dati personali medesimi, **secondo il principio di limitazione del dato**.

c. Accedere agli archivi cartacei e alle banche dati elettroniche esclusivamente per ragioni connesse all'esecuzione delle Sue mansioni, evitando, altresì, di creare nuove banche dati in assenza di espressa autorizzazione della Azienda, **secondo il principio di limitazione del dato**.
d. Custodire i supporti cartacei o informatici, contenenti i dati personali, secondo modalità volte ad evitare che soggetti non autorizzati al trattamento possano accedere ai dati medesimi. Ne consegue, peraltro, che Lei può asportare suddetti supporti cartacei o informatici **esclusivamente** in presenza di autorizzazione espressa della Azienda.
e. Non comunicare i dati personali a soggetti esterni non autorizzati al trattamento, fatta salva l'ipotesi in cui la comunicazione dei dati personali venga richiesta in esecuzione di obblighi di legge. Inoltre l'eventuale comunicazione dei dati personali a specifici destinatari o, addirittura, la diffusione dei dati personali può essere consentita esclusivamente dalla Azienda. In particolare, si precisa che i dati personali possono essere trattati esclusivamente all'interno del territorio italiano, salvo non sia diversamente consentito o autorizzato dalla normativa applicabile o dalle procedure aziendali.
f. In relazione alle banche dati informatiche, custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici, non lasciando incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati personali secondo quanto previsto nel Codice di comportamento aziendale.
g. Osservare le misure di protezione e sicurezza messe in atto dall'Azienda al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati ed individuate nei relativi Regolamenti aziendali ed in particolare nel Codice di comportamento aziendale e nel Regolamento di assegnazione della telefonia fissa e mobile, nonché nel Regolamento di utilizzo dei sistemi informativi aziendali in vigore.
h. In ogni caso Lei s'impegna, compatibilmente con le Sue competenze e conoscenze tecniche, a segnalare alla Azienda, per il tramite del Designato di Struttura e il Referente di Rete Protezione Dati Personali, ogni circostanza che renda necessario od opportuno l'aggiornamento delle misure di sicurezza già in essere al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati medesimi.
i. Fornire immediata comunicazione alla Azienda, secondo quanto previsto da specifica procedura aziendale "Gestione e notifica di violazione di dati personali (Data Breach), in merito alla verificazione ovvero alla presunta verificazione di un incidente sulla sicurezza che possa incidere sulla riservatezza, sull'integrità e sulla disponibilità dei dati personali. A titolo esemplificativo, l'incidente sulla sicurezza potrebbe comportare la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali, ovvero l'accesso accidentale o illegale ai dati personali. Tale comunicazione deve avvenire **nel più breve tempo possibile** dal momento della conoscenza dell'incidente sulla sicurezza, anche al fine di consentire

all'Azienda, nel termine delle 72 ore come previsto dalla norma, di adempiere all'onere di comunicazione dell'eventuale incidente all'Autorità competente.

3. DURATA DELL'ATTO DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

La presente nomina trova applicazione per tutta la durata del rapporto di lavoro fra Lei e la Azienda. Ad avvenuta cessazione del rapporto di lavoro, ogni operazione di trattamento sui dati personali, come individuati nel presente atto, Le sarà preclusa. Resta inteso che l'Azienda si riserva la possibilità di modificare od integrare le istruzioni impartite con il presente atto, al fine di garantire il rispetto della normativa nazionale ed europea in materia di trattamento dei dati personali.

4. ATTIVITA' DI CONTROLLO SULLE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI

Si precisa che l'Azienda si riserva la facoltà di svolgere **controlli periodici** finalizzati a valutare il rispetto dell'obbligo alla riservatezza, dell'integrità, della disponibilità, nonché la conformità delle operazioni da Lei svolte alle istruzioni ricevute e alla normativa in materia di protezione dei dati personali, anche per il tramite del DPO (Responsabile Protezione Dati Personali).

In occasione di suddetti controlli da parte della Azienda, nonché in occasione di eventuale attività ispettiva e di verifica compiuta dall'Autorità competente, Lei è tenuto a prestare la massima collaborazione al fine di garantire il compimento di ogni procedura necessaria a valutare il rispetto della normativa in materia di trattamento dei dati personali.

Il TITOLARE DEL TRATTAMENTO
AULSS 6 EUGANEA
Il Legale Rappresentante pro-tempore

Egr./Egr. a _____,

Premesso che:

- fra Lei e l'Azienda ULSS 6 Euganea (di seguito Azienda) è in corso un rapporto di lavoro;
- in virtù delle specifiche mansioni a Lei affidate, Lei potrà intervenire sugli impianti di elaborazione, contenenti dati personali, dell'Azienda;
- le prestazioni lavorative da Lei effettuate in via ordinaria forniscono idonea garanzia in merito al rispetto dei requisiti di esperienza, di capacità e di affidabilità necessari al fine di assicurare la conformità delle operazioni da Lei poste in essere alla normativa vigente in materia di trattamento dei dati personali, **ivi compreso il profilo relativo alla sicurezza**;
- il presente atto di nomina per **l'Amministratore di Sistema** è adottato in applicazione del Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008 (di seguito "il Provvedimento dell'Autorità Garante"), recepito nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008 e modificato il 25 giugno 2009, nonché nel rispetto della normativa in materia di trattamento dei dati personali come contenuta nel Regolamento UE 2016/679 (di seguito "Regolamento UE") e nel Codice della Privacy (D.Lgs 196/03), in quanto applicabile;
- il Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008 definisce **l'Amministratore di sistema** come la figura professionale **dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP "Enterprise resource planning", le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali**;
- mediante apposito "Atto di autorizzazione al trattamento dei dati personali", Lei è stato preventivamente istruito all'Azienda in merito alle modalità di svolgimento delle operazioni di trattamento sui dati personali, al fine di garantire la liceità e la correttezza delle operazioni di trattamento, nonché la conformità delle operazioni anzidette alla normativa vigente in materia di trattamento dei dati personali; si precisa, pertanto, che il contenuto del presente atto di nomina integra le istruzioni che la Società Le ha già impartito mediante l'atto anzidetto.

Con la presente l'AULSS 6 Euganea La nomina "Amministratore di sistema" in relazione alle operazioni di trattamento di dati personali connesse alla gestione e manutenzione degli impianti di elaborazione dell'Azienda stessa.

In qualità di amministratore di sistema, i Suoi compiti consistono nel:

a) gestire, nel rispetto delle misure di sicurezza applicate dall'Azienda, il sistema informatico in cui risiedono le banche dati dell'Azienda;
b) monitorare il sistema di sicurezza informatico (idoneo a rispettare le prescrizioni dell'art. 32 del Regolamento UE) adottato dalla Società, adeguandolo anche alle eventuali e future norme in materia di sicurezza, attenendosi a specifiche ulteriori aggiornamenti e istruzioni in merito all'entrata in vigore di nuove disposizioni;

c) assegnare e gestire il sistema di autenticazione informatica secondo le modalità ritenute idonee dall'Azienda e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli autorizzati al trattamento dati;
d) procedere alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o autorizzato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per **oltre 6 (sei) mesi**;
e) collaborare con l'Azienda per l'attuazione delle prescrizioni impartite dall'Autorità Garante e comunicare prontamente all'Azienda medesima qualsiasi situazione che possa compromettere il corretto trattamento informatico dei dati personali.

Di seguito è indicato il Suo ambito operativo, nonché le specifiche funzioni a Lei assegnate:
[INDICAZIONE DELL'AMBITO OPERATIVO DELL'AMMINISTRATORE DI SISTEMA E DELLE RELATIVE FUNZIONI]
_____
_____
_____

In particolare, si ricorda che il Provvedimento dell'Autorità Garante obbliga la Società alla "verifica" almeno annuale delle attività da Lei svolte, in qualità di amministratore di sistema, al fine di valutare il rispetto delle misure organizzative, tecniche e di sicurezza predisposte dalla Società in relazione ai trattamenti dei dati personali.
Si precisa, altresì, che il Provvedimento dell'Autorità Garante impone la tracciabilità e la registrazione dell'attività di accesso ai sistemi da parte degli stessi amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi: pertanto, la sua attività di amministratore di sistema verrà monitorata in conformità alle prescrizioni dell'Autorità Garante.

Il TITOLARE DEL TRATTAMENTO
AULSS 6 EUGANEA
Il Legale Rappresentante pro-tempore

Firma per ricevuta e accettazione

_____ _____

Padova, _____