REGIONE TOSCANA
AZIENDA UNITA' SANITARIA LOCALE TOSCANA CENTRO
Sede Legale Piazza Santa Maria Nuova n. 1 – 50122 Firenze

DELIBERA DEL DIRETTORE GENERALE

Numero della delibera	251
Data della delibera	28-02-2020
Oggetto	Procedure aziendali
Contenuto	Sistema Aziendale Privacy:adozione procedura aziendale valutazione di impatto sulla protezione dei dati

Dipartimento	DIREZIONE AMMINISTRATIVA AZIENDALE
Direttore Dipartimento	PESCINI LORENZO
Struttura	SOC AFFARI GENERALI
Direttore della Struttura	CARLINI LUCIA
Responsabile del procedimento	CAGNONI SARA

Conti Economici			
Spesa	**Descrizione Conto**	**Codice Conto**	**Anno Bilancio**
Spesa prevista	**Conto Economico**	**Codice Conto**	**Anno Bilancio**

Estremi relativi ai principali documenti contenuti nel fascicolo		
Allegato	**N° pag.**	**Oggetto**
A	14	Procedura aziendale valutazione di impatto sulla protezione dei dati

"documento firmato digitalmente"

IL DIRETTORE GENERALE
(in forza del D.P.G.R. Toscana n. 33 del 28 febbraio 2019)

Vista la Legge Regionale n. 84/2015 recante "*Riordino dell'assetto istituzionale e organizzativo del Sistema Sanitario Regionale. Modifiche alla Legge Regionale 40/2005*";

Vista la delibera n. 1720 del 24.11.2016 di approvazione dello Statuto aziendale e le conseguenti delibere di conferimento degli incarichi dirigenziali delle strutture aziendali;

Premesso che:
- il Parlamento Europeo ed il Consiglio in data 27/04/2016 hanno approvato il Regolamento Europeo 2016/679 (RGPD) concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, che ha abrogato la direttiva 95/46/CE;
- il suddetto Regolamento è entrato in vigore il 24 Maggio 2016 ed è divenuto definitivamente applicabile in via diretta in tutti gli Stati Membri a partire dal 25 Maggio 2018;
- il D.Lgs 101/2018 (cd. decreto di adeguamento) recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" che è intervenuto modificando il D.Lgs 196/03 ed abrogando, fra l'altro, il Titolo IV relativo ai "soggetti che effettuano il trattamento";*
- il Gruppo di Lavoro articolo 29 sulla protezione dei dati ha adottato in data 4/04/2017 e smi le Linee Guida in materia di valutazione di impatto sui dati ai sensi del regolamento UE 2016/679;
- l'Azienda USL Toscana Centro, è Titolare del trattamento dei dati personali effettuato durante lo svolgimento della propria attività istituzionale come da prima notificazione n. 2016031700221268 (numero iscrizione registro notificazioni);

Richiamati i seguenti atti:
- la deliberazione n. 179 del 30/01/2019 con la quale sono state assunte precise determinazioni inerenti all'assetto organizzativo per la gestione del sistema aziendale privacy al fine di rispettare gli obblighi organizzativi, documentali e tecnici, con l'obiettivo di attuare la piena e consapevole applicazione del nuovo quadro normativo in materia di trattamento dei dati personali perfezionatosi con l'entrata in vigore in data 19/09/2018 del D.Lgs 101/2018 cd. decreto di adeguamento;
- la determina n. 2711 del 24/12/2019 con la quale è stato affidato il servizio di Responsabile della Protezione dei dati personali (RPD) ai sensi del Regolamento UE 2016/679 all'Avv. Michele Morriello;

Considerato che:
- Il regolamento generale sulla protezione dei dati ha disposto che quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate il titolare deve svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo qualora le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;
- Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) del titolare nei confronti dei trattamenti da questi effettuati. Il titolare è, infatti tenuto, non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantisce tale osservanza;

Rilevato che:
- sul portale della privacy sezione cruscotto è stata inserita specifica scheda sulla valutazione di impatto;
- sono stati effettuati 12 edizioni del corso di formazione privacy rivolto ai Referenti del trattamento dei dati ove è stata analizzata, fra l'altro, cosa significa valutazione di impatto del trattamento dei dati personali, come deve essere svolta e le conseguenze sul trattamento degli esiti della valutazione;

Ritenuto, necessario, ratificare con specifica procedura il percorso da attivare in caso di valutazione di impatto sulla protezione dei dati in conformità a quanto stabilito dagli artt.35 e 36 del regolamento UE 2016/679;

Dato atto che:
- la predisposizione della procedura in oggetto è stata condivisa con i componenti del Gruppo di lavoro protezione dei dati coordinato dal Responsabile della Protezione dei Dati, in diversi incontri del gruppo e precisamente nelle date 31/05/2019 ove si è proceduto ad effettuare una simulazione di valutazione di impatto relativamente al trattamento dei dati in ambito di videosorveglianza, nonché nell'incontro del 6/12/ 2019;
- con email del 19/12/2019 è stata inviata al gruppo di lavoro la proposta di procedura come condivisa in sede di incontro, al fine di raccogliere ulteriori osservazioni in merito;

Preso atto che il Direttore della SOC Affari Generali – Dr.ssa Lucia Carlini nel proporre il presente atto attesta la regolarità tecnica ed amministrativa e la legittimità e congruenza dell'atto con le finalità istituzionali di questo Ente, stante anche l'istruttoria, condivisa con il Responsabile della protezione dei dati Avv.Michele Morriello ed effettuata, a cura del Responsabile del Procedimento, Dr.ssa Sara Cagnoni , in servizio c/o la SOC Affari generali.;

Su proposta del Direttore della SOC Affari Generali – Dr.ssa Lucia Carlini;

Acquisito il parere favorevole del Direttore Amministrativo, del Direttore Sanitario e del Direttore dei Servizi Sociali;

DELIBERA

per i motivi espressi in narrativa:

1. **di adottare** la procedura aziendale valutazione di impatto sulla protezione dei dati personali unita al presente atto quale parte integrante e sostanziale sotto la voce di allegato A);

2. **di revocare** ogni e qualsiasi altro atto in contrasto con la presente deliberazione;

3. **di incaricare** il Responsabile del Procedimento di dare informazione del presente atto a tutti i Referenti ed Incaricati del trattamento dei dati anche tramite il Portale della privacy sezione Cruscotto – inserito sul sito intranet previa comunicazione email a tutti i referenti del trattamento dei dati ;

4. **di incaricare** i Referenti del trattamento dei dati ad adempiere alle disposizioni emanate in materia verificando l'applicazione delle stesse da parte del personale assegnato, individuato "incaricato al trattamento dei dati" e fornendogli le istruzioni per l'adozione di comportamenti corretti in materia di tutela della riservatezza e protezione del dato;

5. **di stabilire** che i Referenti e gli Incaricati del trattamento dei dati si impegnano, fra l'altro, a prestare la massima collaborazione nei confronti del Titolare e del Responsabile della Protezione dei Dati fornendo tutte le informazioni richieste al fine di dare compimento agli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali;

6. **di trasmettere**, a cura del Responsabile del procedimento, la presente delibera al Dipartimento Risorse Umane;

7. **di incaricare** la S.O.C Politiche e Relazioni Sindacali, di trasmettere copia del presente atto alle OOSS delle tre Aree negoziali ed alla RSU aziendale ai sensi delle disposizioni vigenti in materia;

8. **di dichiarare** la presente deliberazione immediatamente eseguibile al fine di dare immediato avvio alla procedura in conformità con l'intervenuto quadro normativo di riferimento;

9. **di trasmettere** la presente deliberazione al Collegio Sindacale a norma di quanto previsto dall' art. 42 comma 2, della L.R.T. 40/2005 e ss.mm.ii.

IL DIRETTORE GENERALE
(Dr. Paolo Morello Marchese)

IL DIRETTORE AMMINISTRATIVO
(Dr. Lorenzo Pescini)

IL DIRETTORE SANITARIO
(Dr. Emanuele Gori)

IL DIRETTORE DEI SERVIZI SOCIALI
(Dr.ssa Rossella Boldrini)

Valutazione d

PROCEDURA VALUTAZIONE DI IMPATTO

Data	Redazione	Verifica	Approvazione
29/01/2020	P.O. privacy e supporto Data protection officer – Sara Cagnoni -	**Processo** Responsabile protezione dati - Michele Morriello	Direttore Amministrativo Lorenzo Pescini
		SGQ SOC Affari Generali – Lucia Carlini	

Gruppo di redazione – componenti Gruppo di lavoro protezione dati:

- Emanuele Croppi (Direttore Dipartimento Medicina Generale)
- Ilaria Perigli – Barbara Lazzari (Staff Direttore Generale)
- Daniela Matarrese (Direttore Dipartimento Rete Ospedaliera)
- Alessandro Sergi – Pierluigi Perruccio (Staff Direzione Sanitaria)
- Lucia Carlini (Direzione Amministrativa)
- Alessandro Natali (Dipartimento delle Specialistiche Mediche)
- Giovanni Benelli (Dipartimento delle Specialistiche Chirurgiche)
- Daniela Matteuzzi (Dipartimento Emergenza e Area critica)
- Marco Pezzati (Direttore Dipartimento Materno Infantile)
- Carlo Milandri (Dipartimento Oncologico)
- Martina Boni (Dipartimento di Medicina Fisica e Riabilitazione)
- Grazia Gentilini (Dipartimento di medicina di laboratorio)
- Adriano Viviani (Dipartimento Diagnostica per Immagini)
- Daniele Romeo – Benedetta Novelli (Dipartimento Rete Sanitaria Territoriale)
- Donella Posarelli (Dipartimento Salute mentale e Dipendenze)
- Alberto Anichini (Dipartimento del Farmaco)
- Rosaria Raffaelli – Marco Alaimo (Dipartimento Assistenza Infermieristica ed Ostetrica)
- Riccardo Valencetti (Dipartimento Servizi Tecnico Sanitari)
- Nadia Betti (Dipartimento della prevenzione)
- Mery Cai – Azzurra Staderi (Dipartimento Servizi Sociali)
- Sonny Paccagnini – Sergio Biagini (Dipartimento Risorse Umane)
- Rita Bonciani (Direttore Dipartimento Decentramento)
- Marco Brintazzoli (Direttore Dipartimento Area tecnica)
- Claudia Galanti – Gabriele Bini (Dipartimento Amministrazione, Pianificazione e Controllo di Gestione)
- Sergio Lami (Direttore Dipartimento Interanziendale SIOR)

Parole chiave: procedura, valutazione, impatto

INDICE GENERALE

PREMESSA

Il regolamento generale sulla protezione dei dati, Regolamento Europeo 679/2016 – General Data Protection Regulation (di seguito GDPR) ha un approccio basato sulla **valutazione del rischio.** Con tale valutazione si determina la misura di responsabilità del Titolare del trattamento tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Quindi, il **rischio** inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati.

ART. 1 OGGETTO SCOPO E AMBITO DI APPLICAZIONE

1. La presente procedura disciplina la valutazione d'impatto sulla protezione dei dati - *Data Protection Impact Assessment* (di seguito **DPIA).** Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione (*accountability*) in quanto sostengono il titolare del trattamento non soltanto nel rispetto dei requisiti del regolamento generale sulla protezione dei dati ma anche al fine di dimostrare che sono state adottate misure appropriate per garantire il rispetto del GDPR. Il principale obiettivo è quello di assicurare che il trattamento dei dati personali avvenga nel rispetto delle disposizioni normative quale garanzia di tutela dell'interessato.
2. La presente procedura si applica, obbligatoriamente, in tutti i casi in cui i trattamenti dei dati comportano un rischio elevato per i diritti e le libertà delle persone fisiche come specificato negli articoli seguenti

ART. 2 COSA È LA DPIA

1. La **DPIA** è un processo (art. 35 GDPR) volto a descrivere un trattamento di dati personali per valutarne la necessità e la proporzionalità, nonché i relativi rischi per i diritti e le libertà delle persone fisiche da esso derivanti, allo scopo di approntare misure idonee ad affrontarli.

2. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

ART. 3 QUANDO LA DPIA È OBBLIGATORIA

1. La DPIA è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

2. L'articolo 35 del GDPR ha indicato i criteri in base ai quali si individuano i casi nei quali la DPIA è necessaria:
a) il trattamento determina una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici;
b) il trattamento riguarda le categorie particolari di dati su larga scala;
c) il trattamento riguarda la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

3. Le **Linee Guida relative alla Valutazione d'Impatto** (WP 248 rev.01) hanno precisato ulteriormente i criteri di cui all'art. 35, traducendoli in nove trattamenti (tra i quali la creazione di corrispondenze o combinazioni di insieme di dati, cioé trattamenti ulteriori rispetto alle originarie finalità di dati raccolti da diversi titolari; il trattamento di dati relativi a interessati vulnerabili, come minori, dipendenti, ecc.) utili all'individuazione dei casi di necessità della DPIA.

4. L'Autorità di Controllo (Garante per la protezione dei dati personali) ha predisposto un elenco (adottato con **provvedimento n. 467 dell'11 ottobre 2018**) vincolante ma non esaustivo con il quale ha individuato i trattamenti per i quali è obbligatorio condurre una DPIA. Resta fermo l'obbligo, comunque, di adottare una DPIA laddove ricorrano due o più dei criteri individuati dalle Linee Guida e dall'art. 35 Reg. cit.
Nella tabella sottostante sono elencate le ipotesi di cui al citato provvedimento.

Tabella 1.

1.Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittiveeffettuate anche on-line o attraverso app, relativi ad "*aspetti*

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gliinteressi 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 uncontratto 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 societàdell'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 itrattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, diprevisioni 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 connessialla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidonosull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazionecomporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia dipagamenti).

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 criterinn. 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 deidati 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.
Fonte: Autorità di controllo allegato 1 al provvedimento 467/2019

5. La DPIA è necessaria in presenza di almeno due dei criteri di cui al precedente punto 4 ma, tenendo conto delle circostanze, il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

ART. 4 QUANDO LA DPIA NON È OBBLIGATORIA

1. In base alle Linee Guida del Gruppo Art.29 (WP248) la DPIA non è necessaria per i trattamenti che:

a) non presentano un rischio elevato per diritti e libertà delle persone fisiche;

b) hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;

c) sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es. oggetto, finalità, etc.) non hanno subito modifiche;

d) sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
e) fanno riferimento a norme e regolamenti UE o di uno stato membro, per la cui definizione è stata condotta una DPIA

ART. 5 ESEMPI PER UTILIZZARE I CRITERI PER SOTTOPORRE UN TRATTAMENTO DI DATI A DPIA

1. Gli esempi riportati di seguito illustrano come utilizzare i criteri per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati (DPIA) o meno.

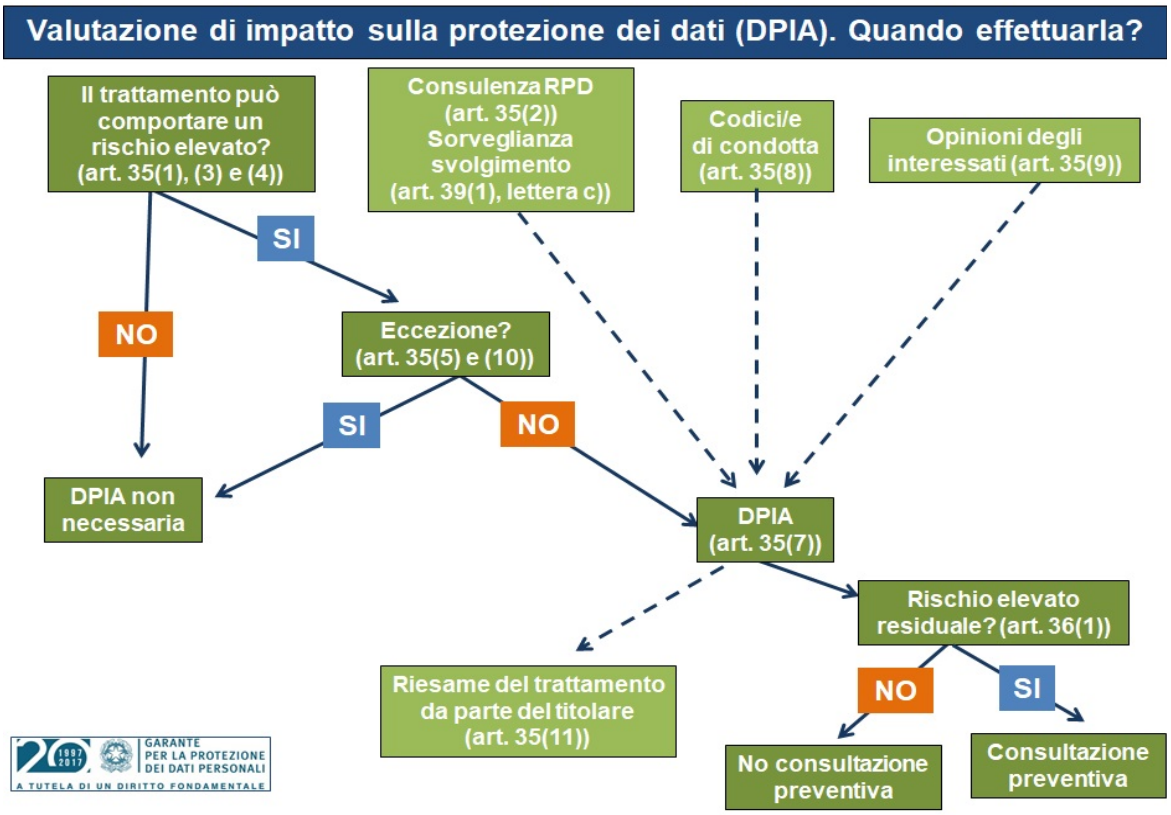
Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili. - Trattamento di dati su larga scala.	SI
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	SI
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	- Dati sensibili. - Dati riguardanti soggetti interessati vulnerabili. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	SI

Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili.	NO

FONTE: Linee Guida del Gruppo di Lavoro Articolo 29 WP248rev.1

ART.6 SCHEMA PER LA DPIA

1. Lo schema seguente (fonte Autorità di controllo) chiarisce il processo di valutazione della obbligatorietà di condurre una DPIA e tutti gli elementi utili a tal fine.



ART. 7 CONTENUTO DELLA DPIA

1. L'art.35 al paragrafo 7, definisce il contenuto minimo (outpu) che deve essere presente nella relazione che documenta la DPIA:

a) la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare;

b) la valutazione della necessità e proporzionalità dei trattamenti;

c) la valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza

e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento.

ART. 8 RUOLI E RESPONSABILITA'

1. Nella tabella che segue sono esplicitati ruoli e responsabilità nel processo DPIA all'interno dell'organizzazione del Titolare del trattamento:

Ruolo aziendale	Responsabilità principali nel processo di DPIA
Titolare del trattamento **(AUSL Toscana Centro)**	Conduce e documenta, di norma, la DPIA. Delega la responsabilità sul processo di DPIA ed all'eventuale consultazione preventiva quando necessaria. Fornisce le risorse organizzative e finanziarie affinché sia possibile la realizzazione del processo di DPIA ed i conseguenti adeguamenti normativi e di sicurezza.
Gruppo di Lavoro Protezione dei Dati (GLPD) (coordinato dal DPO e composto da un rappresentante a livello dipartimentale e da un rappresentante ESTAR)	Coadiuva ed assiste gli attori del processo DPIA: - nella **valutazione preliminare** avente come scopo quello di raccogliere tutte le informazioni necessarie a valutare, in primo luogo, se il trattamento è conforme al regolamento GDPR e, in secondo luogo, comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA - nella **esecuzione** della DPIA: una volta determinata la necessità di procedere ad una DPIA, si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. - **formalizzazione dei risultati**: report finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. - nel **monitoraggio e riesame** (ove necessario).

Referente del trattamento dei dati (Responsabile SOC/SOS autore del processo a cui afferisce il trattamento)	Descrive e documenta il trattamento in tutte le sue caratteristiche È responsabile: - della raccolta delle informazioni sul trattamento ai fini del censimento del trattamento stesso e per la valutazione dei rischi, tra cui sinteticamente: • le categorie di soggetti interessati dal trattamento; • le finalità del trattamento; • le categorie di dati oggetto del trattamento; • le modalità di trattamento; • il luogo / i luoghi di conservazione dei dati trattati; • i processi aziendali che saranno coinvolti nell'attuazione del trattamento; • individuazione dei soggetti esterni che partecipano al trattamento. -della valutazione della conformità: • il trattamento rispetta i princìpi applicabili al trattamento dei dati personali (CAPO II del GDPR) • il trattamento rispetta i diritti degli interessati (CAPO III del Regolamento - dell'obbligatorietà di condurre una DPIA verificando se il trattamento ricade nella casistica di quelli che necessitano obbligatoriamente di una DPIA analizzando principalmente che: • il trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art.35, par. 1); • il trattamento ricade in una delle tipologie di trattamenti per le quali non è richiesta una DPIA(Art.35, par. 5); • il trattamento risulta già normato di diritto (Art.35, par. 10).: - della raccolta delle informazioni per l'analisi dei rischi in grado di caratterizzare il trattamento e le sue

	peculiarità; - della valutazione dei rischi: la DPIA è di norma sviluppata quale valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromettere un asset; - della valorizzazione delle contromisure esistenti che, associate alle minacce, consentono di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile precedentemente definito. Qualora il valore di rischio ricada entro la soglia di accettabilità, il trattamento potrà essere definito sufficientemente sicuro e si potrà procedere alla formalizzazione dei risultati. Nel caso in cui invece il valore di rischio residuo risulti sopra la soglia di accettabilità si dovrà procedere a rivedere le contromisure applicate alzando il livello di implementazione delle contromisure esistenti oppure introducendo nuove contromisure più efficaci a protezione del trattamento analizzato. In tal caso il valore di rischio sarà ricalcolato ottenendo quindi un nuovo valore di rischio residuo a seguito della applicazione delle nuove contromisure che a questo punto concorreranno alla preparazione del piano di trattamento dei rischi. - del piano di trattamento dei rischi: Tutte le informazioni raccolte ed elaborate durante il processo di analisi dei rischi devono essere formalizzate a supporto della realizzazione del piano di trattamento. Nel caso in cui il trattamento preveda l'impiego di Sistemi Informatici esterni, si confronta con i Responsabili che forniscono il servizio. In caso di un trattamento esistente che presenta un cambiamento del profilo di rischio coordina le attività per l'aggiornamento della DPIA

Rappresentante del Dipartimento/Area (valutatore del processo a cui afferisce il trattamento)	Coordina le attività necessarie alla DPIA. Segnala al Titolare e al DPO il nuovo trattamento e/o la modifica di un servizio esistente nel caso di modifica del profilo di rischio. Valuta il complessivo processo DPIA
Ufficio privacy (validatore del processo a cui afferisce il trattamento)	Monitora lo svolgimento della DPIA verificando 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.
Responsabile della protezione dei Dati (DPO)	Supervisiona l'intero processo DPIA esprimendo parere conclusivo di conformità al GDPR. È responsabile del processo di consultazione preventiva e funge da interfaccia per l'Autorità di Controllo. Qualora l'analisi a cui si è giunti al termine del processo DPIA e riportata all'interno del Report conclusivo, indichi che il trattamento possa presentare un rischio elevato, in assenza di misure adottabili dal Titolare del trattamento in grado di attenuare il rischio, il Titolare del trattamento, prima di procedere al trattamento, deve consultare l'Autorità di Controllo. La consultazione preventiva, come indicato all'interno dell'art. 36 par. 3 deve contenere alcune informazioni fondamentali fra cui: • ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; • le finalità e i mezzi del trattamento previsto; • le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; • i dati di contatto del titolare della protezione dei dati; • la valutazione d'impatto sulla protezione dei

	dati di cui all'articolo 35; • ogni altra informazione richiesta dall'autorità di controllo. • i dati di contatto del DPO. Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo, il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo. L'autorità a questo punto ha 8 settimane, prorogabili una sola volta di altre 6 settimane, per concludere la consultazione. Nel caso in cui non dovesse pervenire alcuna risposta entro il termine di otto settimane, il silenzio assenso dell'Autorità potrà quindi essere interpretato come una implicita conferma che non sono stati ravvisati motivi di contrasto tra il trattamento che si intende iniziare ed il GDPR. Se invece l'Autorità ha ravvisato una possibile violazione del regolamento in quanto per il trattamento in questione il Titolare non abbia identificato o attenuato sufficientemente il rischio, la medesima potrà fornire un parere scritto al Titolare del trattamento in tal senso.
Rappresentante all'interno del GLPD della SOC Progetti Tecnologici	Supporta il processo di DPIA con riguardo alle esigenze di sicurezza. Coordina l'implementazione delle misure di sicurezza necessarie emerse da DPIA in carico ad ESTAR funzioni ICT
Rappresentante all'interno del GLPD di ESTAR funzioni ICT	Supporta il processo di DPIA fornendo competenze ed informazioni relativamente agli aspetti tecnici di competenza Fornisce le informazioni di analisi dei rischi generali Implementa le modifiche richieste in termini di soluzioni di sicurezza

ART. 9 SANZIONI

1. Nelle ipotesi di mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa, di

esecuzione in maniera errata di detta valutazione oppure di mancata consultazione dell'autorità di controllo laddove richiesto, il Titolare del trattamento può essere destinatario di una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di Euro (art. 83, par. 4, GDPR).
È fatto obbligo a chiunque competa di osservare le disposizioni di cui alla presente procedura. La violazione delle stesse è fonte di responsabilità disciplinare.

ART. 10 RIFERIMENTI NORMATIVI

1. Regolamento (UE) 2016/679 del Parlamento Europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in particolare Sezione 3, art. 35 (Valutazione d'impatto sulla protezione dei dati e considerando nn.84,da 89 a 93, 95) art. 36 (Consultazione preventiva e considerando nn.da 94 a 96).

2. D.Lgs. 196/2003 Codice per la protezione dei dati personali come "adeguato" con D. Lgs. 10 agosto 2018 n. 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)".

3. Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248 rev.01

4.Provvedimento del Garante n. 467 del 11 ottobre 2018: Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto

ART. 11 MODALITA E INDICE DI REVISIONE

1. La revisione si effettua per intervenute modifiche normative, per cambiamenti assetti organizzativi e per successive valutazioni corredate di adeguate e sostanziali motivazioni

Revisione n°	Data emissione	Tipo modifica	titolo
0	29/01/2020	Prima emissione	

2. Per la conduzione della DPIA, ordinariamente, viene utilizzato il software open source per la valutazione di impatto messo a disposizione dal CNIL (autorità di controllo francese) segnalato anche dall'Autorità di Controllo italiana.

ART. 12 LISTE DI DIFFUSIONE

1.Tutto il personale con ruolo di "incaricato del trattamento dei dati" dell'Azienda USL Toscana Centro mediante inserimento della procedura sulla rete intranet - Portale della Privacy - sezione "Cruscotto";

2.Tutti i Direttori di struttura organizzativa e altro personale con ruolo di "Referente del trattamento dei dati" mediante comunicazione email.