REGIONE ABRUZZO
Azienda Sanitaria Locale n. 2 LANCIANO–VASTO–CHIETI
Via Dei Vestini s.n.c. – Chieti "Palazzina N"
C.F. e P. Iva 02307130696

DELIBERAZIONE

DEL

DIRETTORE GENERALE

N. 997 **DEL** 10 NOV. 2020

DELIBERA IMMEDIATAMENTE ESECUTIVA

Oggetto: Adozione procedura per la gestione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA- Data Protection Impact Assessment) art 35 e 36 Regolamento UE n. 679/16.

IL DIRETTORE GENERALE

Thomas Schael, nominato con delibera della Giunta Regionale d'Abruzzo n. 543 del 11 Settembre 2019 ai sensi del vigente Decreto Legislativo n. 502 del 30 dicembre 1992 e successive modifiche ed integrazioni;

VISTA l'allegata proposta di deliberazione di pari oggetto del Dirigente Responsabile della U.O.S.D. Sistema Informazione, Comunicazione e Marketing, datata 10/11/2020 ;

DATO ATTO dell'attestazione di regolarità e legittimità dell'atto da parte del Dirigente della predetta Unità Operativa, come acquisita in calce alla proposta medesima;

ACQUISITI i pareri espressi ed attestati in calce dal Direttore Amministrativo Aziendale e dal Direttore Sanitario Aziendale, per quanto di rispettiva competenza;

D E L I B E R A

di fare integralmente propria la menzionata proposta di deliberazione, che forma parte integrante e sostanziale del presente atto e di disporre in conformità della stessa.

Parere favorevole _____ **Il Direttore Amministrativo Aziendale**
(Giulietta Capocasa)

Parere favorevole _____ **Il Direttore Sanitario Aziendale**
(Angelo Muraglia)

IL DIRETTORE GENERALE
(Thomas Schael)

Proposta di deliberazione per il Direttore Generale

OGGETTO: Adozione procedura per la gestione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA- Data Protection Impact Assessment) artt. 35 e 36 Regolamento UE 2016/679.

Visto :

-il 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 - GDPR);

-il d.lgs. 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", come integrato con le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101, 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

Considerato che il GDPR dispone, all'art.35, che "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" e che in particolare, l'esecuzione della DPIA è richiesta nei casi di cui al par 3 del menzionato articolo;

Considerato altresì che a mente del già citato art 35 GDPR "la valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione";

Tenuto conto del fatto che l'art 36 GDPR stabilisce che "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio";

Ritenuto, pertanto, necessario ed opportuno predisporre una procedura, con relativo modello, che si allega al presente atto deliberativo di cui costituisce parte integrante e sostanziale;

Acquisito il parere favorevole del DPO/RPD aziendale sull'adottanda procedura;

PROPONE DI DELIBERARE QUANTO SEGUE:

per tutti i motivi esplicitati in narrativa e che debbono intendersi per integralmente riportati e trascritti nel presente dispositivo,

-Di adottare la procedura per la gestione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA- Data Protection Impact Assessment) art 35 e 36 Regolamento UE n. 679/16, allegata come parte integrante e sostanziale al presente atto deliberativo quale procedura aziendale;

-Di dichiarare il presente provvedimento immediatamente esecutivo;

-Di pubblicare il presente atto deliberativo sul sito aziendale nella sezione privacy;

-Di trasmettere copia del presente atto con l'allegata procedura alla UOC Affari Generali e Legali perché ne curi la pubblicazione sull'Albo Pretorio on-line di questa ASL, al DPO/RPD, alla U.O.C. Informatica e Reti, alla UOC Ingegneria Clinica e a tutte le UU.OO dell'area Medico-Veterinaria, Sanitaria, Amministrativa, Tecnica e Professionale Aziendali, alle Direzioni Mediche Ospedaliere, ai NOD, al Dipartimento di Prevenzione, ai Dipartimenti Sanitari ed al Collegio Sindacale.

La presente deliberazione consta di n. 5 pagine e di n. 1 allegato.

L'Istruttore
Collaboratore Amministrativo
(Gaspare Staniscia)

Data 10/11/2020

Firma

Il Dirigente Responsabile dell'U.O.proponente
che attesta la legittimità e la regolarità dell'atto
(Giustinantonia Chieffo)

Data 10/11/2020

Firma

SCHEDA CONTABILE

PRIMA PARTE (A CURA DELLA UO PROPONENTE L'ATTO DELIBERATIVO)

Importo spesa disposta col presente atto (iva inclusa)	Aliquota IVA	conto di COGE in cui la spesa è stata prevista	Importo eventualmente non ricompreso negli stanziamenti di bilancio	descrizione della modalità di finanziamento dell'importo eccedente	Fonti di finanziamento finalizzate-progetti obiettivo e/o fondi finalizzati (Indicare estremi atto Regionale e Aziendale di concessione/destinazione del finanziamento, ecc.)
Il presente documento non comporta spese				Riduzione spesa già stanziata (indicare quale)	
				Contributo (vedi colonna successiva)	

Il Direttore della U.O. proponente _____

Data _____

SECONDA PARTE (A CURA DELLA UO BILANCIO)

CONTO DI CO.GE.		CAPIENZA VOCE DI CONTO (Indicare Si/No e Importo)	CAPIENZA FONDI FINANZIAMENTO SPECIFICO (Indicare L.P. o fondo specifico di finanziamento)	IMPORTO NON COPERTO (Indicare Importo fuori previsione di Bilancio)

Si attesta, previa verifica, che il costo derivante dal presente atto TROVA/NON TROVA (barrare la voce che non interessa) capienza all'interno del budget assegnato sul C.E. del bilancio_____ (indicare anno), come da tabella che precede.

Il Dirigente della U.O.C. Contabilità e Bilancio _____

Data _____

Della suestesa deliberazione viene iniziata la pubblicazione il giorno

10 NOV. 2020 con prot. n. 65793

all'Albo della ASL per rimanere ivi affissa per 15 giorni consecutivi ai sensi della L. n. 267/2000 e della L.R. n. 28/1992.

o La suestesa deliberazione diverrà esecutiva a far data dal decimo giorno successivo alla pubblicazione.

x La suestesa deliberazione è stata dichiarata "immediatamente eseguibile".

Il Funzionario preposto

Procedura

per la Gestione delle Valutazioni di Impatto sulla Protezione dei Dati (DPIA – Data Protection Impact Assessment)

della ASL 2 Lanciano Vasto Chieti

in base a quanto previsto dal

art. 35 e 36 del Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) e D.Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali

Sommario

1. Introduzione

La normativa vigente in termini di Protezione dei Dati Personali, costituita dal Regolamento UE 679/2016 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento") e dal D. Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice") come modificato dal D.Lgs. 101/2018, ha l'obiettivo di proteggere i dati personali degli interessati al fine di evitare che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati. Considerato il contesto operativo dell'Azienda Sanitaria, tali problematiche sono di notevole rilevanza.

Le tipologie di dati personali oggetto dei trattamenti effettuati, e che potrebbe effettuare, dall'Azienda sono costituiti sia da dati personali (ad esempio dati anagrafici, recapiti, identificativi di tessera sanitaria, codici fiscali, ecc...) che da "particolari categorie di dati personali" ai sensi dell'art. 9 del GDPR e dati personali relativi a condanne penali e reati, ai sensi dell'art. 10 del GDPR, che possono rientrare nelle tipologie di cui all. 1 del provvedimento n. 467 del 11/10/2018 del Garante Privacy.

La ASL 2 di Lanciano Vasto Chieti (di seguito "ASL") predispone il presente documento nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati.

2. Scopo e campo di applicazione

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle Valutazioni di Impatto sulla Protezione di Dati e delle relative indicazioni operative per poter procedere con la rilevazione, la valutazione e l'identificazione delle misure di sicurezza necessarie per l'esecuzione di un trattamento nel rispetto di quanto previsto dagli artt. 35 e 36 del Regolamento UE 679/2016; viene inoltre valutata la necessità di dover procedere con la comunicazione preventiva all'Autorità Garante per la Protezione dei Dati Personali nei casi previsti dalla normativa.

La procedura si applica nel caso in cui dovesse manifestarsi l'esigenza di:

- una variazione/dismissione di un trattamento esistente che abbia rilevanza in materia di protezione dei dati personali o
- l'attivazione di un nuovo trattamento di dati personali.

La presente procedura definisce le modalità di esecuzione della Valutazione di Impatto sulla Protezione dei Dati, con particolare riguardo agli aspetti organizzativi rimandando alle specifiche normative/linee guida settoriali eventuali precisazioni relative all'esecuzione tecnica delle valutazioni.

3. Definizioni

Le seguenti definizioni sono di utilità per poter dare le risposte opportune nell'ambito del questionario in base all'art. 4 del Regolamento:

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

«trattamento»: 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;

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

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

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

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

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: 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;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«violazione dei dati personali»: 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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«evento sulla sicurezza delle informazioni»: occorrenza identificata di uno stato di un sistema, servizio o della rete che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza

«incidente sulla sicurezza delle informazioni»: evento singolo o serie di eventi sulla sicurezza delle informazioni indesiderati o imprevisti che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni

«DPO»: Data Protection Officer o Responsabile della Protezione Dati

4. Normativa di Riferimento

I riferimenti normativi e prescrizioni per la redazione della Valutazione di Impatto sulla Protezione dei Dati (DPIA) sono i seguenti:

- Regolamento UE 679/2016 negli articoli specifici 35 e 36.
- Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)
- EDPS, Accountability on the ground Part I: Records, Registre and when to do Data Protection Impact Assessment
- Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679
- Circolare AgID 2/2017
- Controlli applicabili ISO 27001
- Provvedimenti del Garante "Amministratore di Sistema"

4.1 Articolo 35 GDPR - Valutazione d'impatto sulla protezione dei dati

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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una 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) il 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; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), 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.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

4.2 Articolo 36 GDPR - Consultazione preventiva

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.
3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:
a) 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;
b) le finalità e i mezzi del trattamento previsto;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
d) ove applicabile, i dati di contatto del titolare della protezione dei dati;
e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
f) ogni altra informazione richiesta dall'autorità di controllo.
4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.
5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

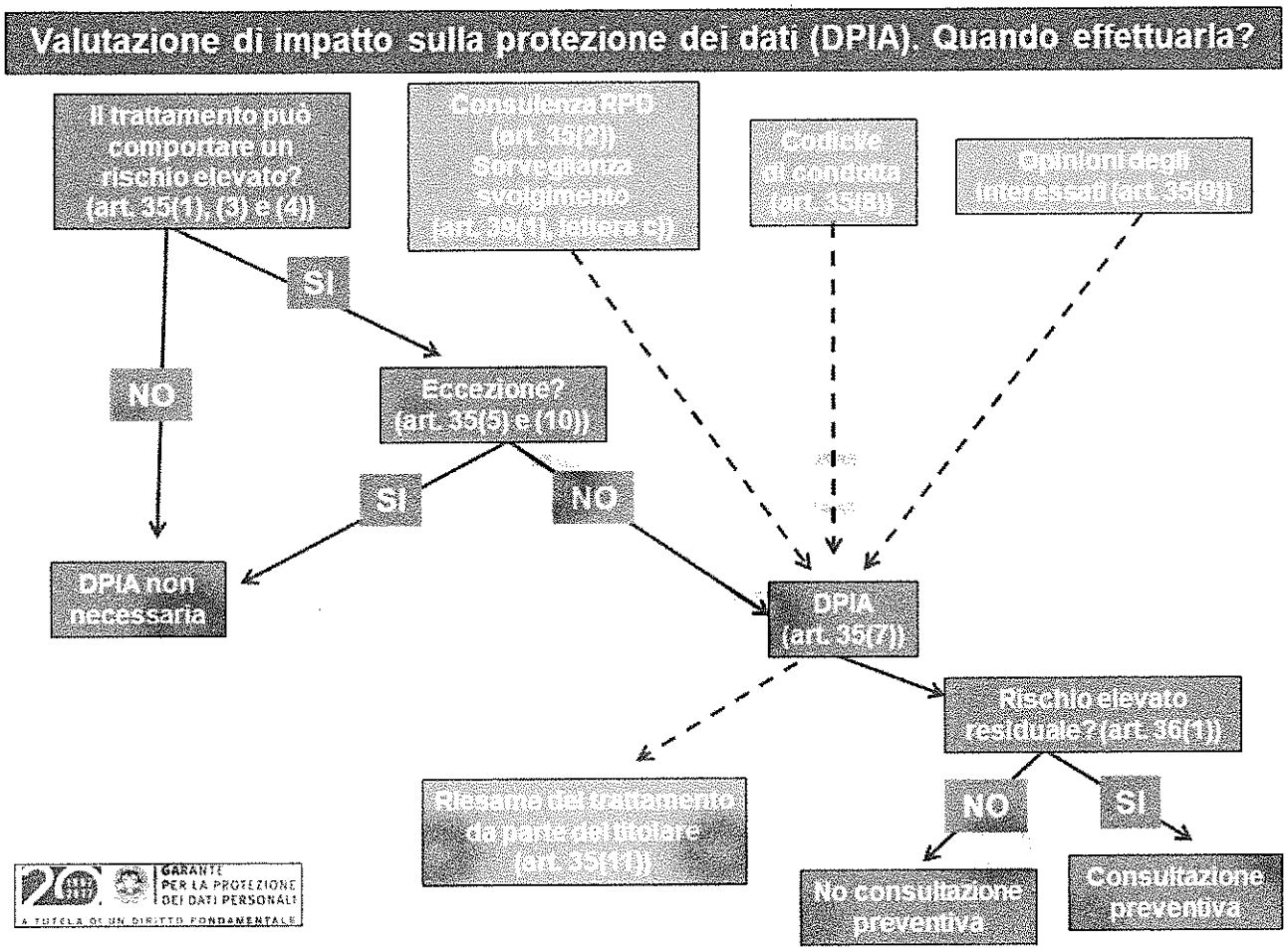
5. Definizione dei trattamenti da sottoporre a DPIA

La definizione dei trattamenti da sottoporre a DPIA si basa sul seguente elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – individuato con il provvedimento n. 467 dell'11 ottobre 2018.

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.

Come definito nelle linee guida WP 248 rev.01, nella maggior parte dei casi, il titolare del trattamento di concerto con il Team DPIA può considerare che un trattamento **che soddisfi due delle sopraelencate tipologie** debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. In generale, il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.
Tuttavia, in alcuni casi, il titolare del trattamento, sentito il Team DPIA, può ritenere che un trattamento **che soddisfa soltanto uno delle tipologie di cui sopra** richieda una valutazione d'impatto sulla protezione dei dati.
Quanto sopra è riassunto schematicamente nella seguente figura.



6. Soggetti coinvolti nel processo di effettuazione di una DPIA

Il Titolare del trattamento ha ritenuto opportuno definire che la redazione della valutazione d'impatto sia da svolgere a cura del Team DPIA aziendale costituito dai soggetti di seguito rappresentati.

La DPIA prevede tre fasi di elaborazione:

- Redazione, a cura del Team DPIA
- Valutazione, a cura del RPD
- Validazione, a cura del Titolare

6.1 Team DPIA

Il Team DPIA è una entità multidisciplinare attivata dal Soggetto Autorizzato al Trattamento con Delega (SATD), ovvero Direttore/Dirigente di UUOO, che svolge il ruolo fondamentale sia nella fase segnalazione di variazione/introduzione di un trattamento di dati personali che nella fase di valutazione della fattibilità delle misure proposte da parte del Team DPIA.

La composizione del Team è costituita in maniera stabile dai referenti delle strutture organizzative direttamente coinvolte nella gestione della Protezione dei Dati Personali (UOC Informatica e Reti e Ufficio Privacy) e opzionalmente, su richiesta da parte dei componenti di base del Team, da ulteriori referenti.

Team DPIA		
Funzione	**Competenza**	**Partecipazione**
SATD	Conoscenza del trattamento e delle specifiche tecniche degli asset di supporto.	componente di base che attiva la procedura
UOSD SICM/ufficio privacy	Ufficio competente per la gestione degli adempimenti Privacy aziendali	Componente di base che coordina la procedura
UOC Informatica e Reti	conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	Componente di base
UOC Ingegneria Clinica	Conoscenza delle attrezzature Sanitarie di trattamento dati	Componente di base

Il Team DPIA deve assicurare un'adeguata analisi del trattamento in esame, oltre a fornire tutte le necessarie indicazioni per l'identificazione delle minacce, vulnerabilità e delle misure per il contrasto dei possibili eventi avversi in relazione al mancato rispetto dei principi di trattamento, diritti e libertà degli interessati.

La documentazione che scaturisce da questa attività dovrà contenere, almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

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

d) le misure previste per affrontare i rischi, includendo le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento.

Opportunamente, in caso di attività di trattamento che coinvolgano organizzazioni che operino in nome e per conto del Titolare, il Team DPIA dovrà ricorrere al coinvolgimento dei Responsabili del Trattamento con la somministrazione di schede tecniche valutative del servizio e richiesta di informazioni suppletive che si ritengano necessarie per la redazione della Valutazione d'Impatto.

Opzionalmente, in base alle necessità, la UOSD SICM/Ufficio Privacy coordinatore può integrare ulteriore personale nel team se ritenuto utile nell'ambito delle analisi e valutazioni effettuate per la DPIA.

Se del caso, il Team DPIA raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

6.1.1 Obiettivi di una D.P.I.A.

La D.P.I.A. deve conseguire i seguenti obiettivi:

a) individuare con precisione i rischi elevati che si associano al trattamento che ci si prefigge di realizzare, tenendo conto della natura dei dati e del trattamento, dell'ambito, del contesto e degli scopi del trattamento stesso e delle fonti di rischio;

b) valutare i rischi elevati previamente individuati, in particolare le fonti, la natura e le peculiarità, la probabilità nonché l'eventuale gravità del rischio stesso;

c) individuare quali misure adottare per mitigare i rischi elevati, adeguate in termini di tecnologie disponibili e costi di implementazione e proporre tali misure;

d) documentare i risultati, le valutazioni e le misure adottate (o non adottate motivandole) in modo da poter dimostrare la conformità ai requisiti fissati dal GDPR.

6.2 Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati ha il compito di valutare l'elaborazione effettuata dal Team DPIA.

In caso di valutazione negativa il RPD rinvia la DPIA, con le dovute osservazioni, al Team.

In casi di valutazione positiva il RPD trasmetterà l'esito di tale verifica al Titolare.

6.3 Titolare del trattamento

Il Titolare del Trattamento ha il compito di validare la valutazione o di richiedere, in caso di rischio residuo elevato, un parere consultivo all'autorità Garante per la Protezione dei Dati Personali.

Il Titolare del trattamento si riserva la facoltà di far eseguire al SATD richiedente un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati, almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

7. Descrizione del Processo di Valutazione di Impatto (DPIA)

Il processo di esecuzione della DPIA si compone delle seguenti fasi:

7.1 Fase 1 – Rilevazione di un nuovo trattamento o modificato da parte del SATD

Il processo viene avviato in base alla segnalazione all'Ufficio Privacy, da parte del Soggetto Autorizzato al Trattamento con Delega competente per lo specifico trattamento, in base ad una modifica dello stesso o all'introduzione di un nuovo processo di trattamento di dati personali.

Il SATD fornirà al Team DPIA una serie di informazioni in accordo con art. 30 GDPR, relative al trattamento (descrizione generale) secondo i seguenti punti:
CONTESTO

- Descrizione generale
- Responsabilità (interne ed esterne)

- Caratteristiche
- Specifiche tecniche asset di Supporto

PRINCIPI FONDAMENTALI

- Finalità e scopi
- Legittimità
- Dati e ciclo di vita
- Misure di sicurezza tecnico-organizzative esistenti

MISURE ESISTENTI E/O PIANIFICATE

- Informazioni
- Esercizio diritti
- Obblighi dei responsabili

7.2 Fase 2 – Verifica della documentazione

Il Team DPIA procederà alla verifica della congruità della documentazione ricevuta, riservandosi se del caso di acquisirne ulteriore e integrativa da parte del SATD richiedente.

7.3 Fase 3 – Esecuzione della valutazione di impatto e misure di sicurezza

Definite la documentazione e le informazioni, il Team DPIA si occuperà di effettuare la valutazione di impatto (DPIA) secondo le seguenti attività operative:

a) **Attività di verifica e inserimento informazioni**

- Definizione del contesto, con la valorizzazione delle seguenti informazioni:
  - Panoramica del trattamento, che permette di individuare e presentare l'oggetto della valutazione
  - Dati, processi e risorse a supporto, che permettono di descrivere nei dettagli il trattamento in oggetto richiesto
- Definizione dei Principi Fondamentali, con la redazione delle due sottosezioni:
  - Individuazione degli strumenti che garantiscono la necessità e la proporzionalità del Trattamento
  - Individuazione delle misure per la protezione dei diritti degli interessati

Per lo svolgimento di tale attività saranno necessarie le informazioni richieste all'art. 30 del GDPR, le specifiche degli asset e delle risorse coinvolti, le procedure, le norme di riferimento.

b) **Attività di definizione dei rischi**

- Individuazione dei rischi con la valorizzazione delle seguenti informazioni:
    - Definizione delle misure esistenti o pianificate ai fini della sicurezza dei dati
    - Individuazione minacce che possano minare la riservatezza dei dati
    - Individuazione minacce che possano minare l'integrità dei dati
    - Individuazione minacce che possano minare la disponibilità dei dati
- Riepilogo dei rischi con visione globale e sintetica degli effetti prodotti dalle misure sulle componenti di rischio che esse contribuiscono a mitigare.

Per lo svolgimento di tale attività saranno necessarie le attività di verifica degli asset coinvolti nell'attività di trattamento, la descrizione dell'infrastruttura tecnologica e logistica a supporto, le procedure e le misure adottate e/o pianificate.

A titolo esemplificativo, ma non esaustivo, possono essere prese a riferimento:

- Controlli AgID circolare 2/2017
- Controlli applicabili ISO 27001
- Check list di controllo appropriate
- Provvedimento del Garante "Amministratore di Sistema"
- Documentazione e procedure di gestione dell'infrastruttura tecnologica
- Documentazione e procedure di gestione delle apparecchiature elettromedicali

c) **Attività di convalida**

- Mappatura del rischio con il confronto del posizionamento del rischio prima e dopo l'applicazione delle misure aggiuntive
    - Piano di azione con la valutazione dei Controlli di Sicurezza
    - Valutazione del Rischio residuo con identificazione delle misure di sicurezza tecnico-organizzative ritenute adeguate

Per lo svolgimento di tale attività saranno necessarie il completamento delle precedenti attività e l'applicazione delle misure per la riduzione del rischio

7.4 Fase 4 – Valutazione della fattibilità da parte del SATD

Completata la valutazione di impatto da parte del Team DPIA, il SATD verificherà la fattibilità delle misure tecnico-organizzative indicate dal Team e il rischio residuo. In caso di riscontro positivo si procede con la

fase successiva, se negativo, adeguatamente motivato da parte del SATD, la valutazione viene rimandata al Team per una successiva fase di elaborazione basandosi sull'acquisizione di nuovi elementi.

Nel caso in cui il Team, nonostante il riscontro negativo del SATD, confermi o modifichi l'elaborazione, la valutazione dovrà essere sottoposta al Responsabile della Protezione Dati per la necessaria valutazione.

7.5 Fase 5 – Valutazione da parte del RPD

L'elaborazione finale del Team, corredato del riscontro del SATD competente per il trattamento oggetto di analisi, deve essere sottoposta, per il tramite dell'Ufficio Privacy, al Responsabile della Protezione dei Dati, il quale esprimerà un proprio parere che comunicherà al titolare unitamente all'elaborazione effettuata.

7.6 Fase 6 – Validazione da parte del Titolare del Trattamento

La valutazione d'impatto effettuata dal Team DPIA, unitamente ai pareri del SATD e valutazione del Responsabile della Protezione dei Dati, sarà trasmessa - per il tramite dell'Ufficio Privacy - al Titolare del Trattamento che avrà il compito di apporre la validazione finale al rischio residuo e l'emissione della valutazione.

Nel caso in cui fosse presente un rischio residuo elevato e non "comprimibile", il Titolare – qualora decida di attivare il trattamento in parola - dovrà richiedere opportuno parere all'Autorità Garante Privacy secondo quanto previsto dall'art. 36 del Regolamento UE 679/2016.

8 Strumenti e risorse

Il Team DPIA per la redazione della valutazione d'impatto utilizzerà il format di cui all'allegato 1 ovvero potrà acquisirne altri ritenuti altrettanto validi ed efficaci.

Valutazione di impatto

(*data protection impact assessment* - DPIA)

sulla protezione dei dati personali

redatta ai sensi dell'art. 35 del Reg. UE 679/2016 e sulla base delle Linee Guida del 4/10/2017 del Working Party Art. 29.

NOME AZIENDA

DATA EMISSIONE	
REDATTORE	
VERIFICATORE INTERNO	
VALIDATORE	
VERSIONE	
DATA REVISIONE	

DEFINIZIONE DEL CONTESTO

Criteri indicativi di rischio elevato

☐ **VALUTAZIONE O ASSEGNAZIONE DI UN PUNTEGGIO** Trattamenti **valutativi** o di ***scoring*** su larga scala Trattamenti che comportano la **profilazione** degli interessati, lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti: • rendimento professionale • situazione economica • salute • preferenze o interessi personali • affidabilità o comportamento • ubicazione o spostamenti	
☐ **PROCESSO DECISIONALE AUTOMATIZZATO** Trattamenti automatizzati finalizzati ad assumere decisioni che producono "**effetti giuridici**" o che **incidono "in modo analogo significativamente"** sull'interessato, comprese le decisioni che impediscono di: • esercitare un diritto • avvalersi di un bene o di un servizio di continuare ad essere parte di un contratto in essere	
☐ **MONITORAGGIO SISTEMATICO** Trattamenti che prevedono un utilizzo sistematico di dati per **osservazione, monitoraggio o controllo** degli interessati, compresa: • raccolta di dati attraverso **reti**, effettuati anche on-line o attraverso app; • sorveglianza sistematica su larga scala di una **zona accessibile** al pubblico • 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; • 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.	
☐ **TRATTAMENTI SU LARGA SCALA DI DATI AVENTI CARATTERE ESTREMAMENTE PERSONALE** Si fa riferimento, fra gli altri, a: • dati connessi alla vita familiare o privata (quali i dati relativi alle **comunicazioni elettroniche** dei quali occorre tutelare la riservatezza), • dati che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'**ubicazione**, la cui raccolta mette in gioco la libertà di circolazione)	 

• dati 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).	
☐ **CONTROLLO A DISTANZA DEI LAVORATORI** 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	
☐ **DATI RELATIVI A INTERESSATI VULNERABILI** Trattamenti **non occasionali** di dati relativi a soggetti **vulnerabili**: • minori • disabili • anzianì • infermi di mente • pazienti • richiedenti asilo • dipendenti	   
☐ **USO INNOVATIVO O APPLICAZIONE DI NUOVE SOLUZIONI TECNOLOGICHE O ORGANIZZATIVE** 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.	
☐ **SCAMBIO DI DATI** Trattamenti che comportano lo scambio tra **diversi titolari** di dati su **larga scala** con modalità telematiche.	
☐ **INTERCONNESSIONE, COMBINAZIONE, RAFFRONTO** 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***).	
☐ **DATI SENSIBILI O GIUDIZIARI** Trattamenti di categorie **particolari** di dati oppure di dati relativi a **condanne penali e a reati** interconnessi con altri dati personali raccolti per finalità diverse.	 

☐ **DATI BIOMETRICI** Trattamenti **sistematici** di **dati biometrici**, trattati per identificare univocamente una persona fisica, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	
☐ **DATI GENETICI** Trattamenti **sistematici** di **dati genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.	
☐ **Nessuno** DPIA volontaria secondo il principio di *accountability*.	

Descrizione del trattamento dei dati personali oggetto di DPIA:

_____
_____
_____
_____

_____
_____
_____
_____

Finalità del trattamento

- _____
- _____
- _____
- _____
- _____
- _____
- _____

Categorie di soggetti interessati dal trattamento

☐ Pazienti ☐ Dipendenti

☐ Collaboratori

☐ Clienti

☐ Visitatori

☐ *Prospect*

☐ Fornitori

☐ Partecipanti a studi clinici

☐ Utenti

☐ Candidati

☐ Associati

☐ Altro_____

Titolare/i del trattamento

_____
_____
_____
_____

Responsabile/i del trattamento

- _____
- _____
- _____
- _____
- _____
- _____
- _____

DATI

Descrizione dei dati trattati	☐ Nome	☐ Stato di salute
	☐ Cognome	☐ Stato di salute di un familiare
	☐ Indirizzo postale	☐ Vita sessuale
	☐ Città di residenza	☐ Stato di famiglia/dati relativi alla famiglia
	☐ CAP	☐ Curriculum
	☐ Sesso	☐ Esperienze lavorative/occupazione attuale
	☐ Età	☐ Istruzione e cultura
	☐ Indirizzo mail	☐ Beni, proprietà e possesso

	☐ Indirizzo PEC	☐ Dati economici/patrimoniali
	☐ Numero di telefono fisso	☐ Coordinate bancarie
	☐ Numero di cellulare	☐ Ubicazione geografica/localizzazione
	☐ Data di nascita	☐ Impronte digitali per sottoposizione a rilevazione
	☐ Codice Fiscale	☐ Iride per sottoposizione a scansione
	☐ Codice identificativo univoco	☐ Volto per sottoposizione a riconoscimento facciale
	☐ Origini razziali o etniche	☐ Firma grafometrica
	☐ Convinzioni religiose	☐ Condanne penali o reati
	☐ Adesione a sindacati	☐ Altro_____
	☐ Convinzioni filosofiche	☐ Altro_____
	☐ Carta di identità	☐ Altro_____
	☐ Patente di guida	☐ Altro_____
	☐ Passaporto	☐ Altro_____
	☐ Tessera sanitaria	☐ Altro_____
	☐ Carta di credito	☐ Altro_____
	→NOTE: _____	
	_____	
	_____	
	_____	

Il Titolare aderisce a un Codice di condotta?	→SPECIFICARE:
☐**SI** ☐**NO**	

È stato richiesto il parere agli interessati?	→MOTIVARE L'EVENTUALE ASSENZA DEL PARERE DEGLI INTERESSATI:
☐**SI** ☐**NO**	

RISPETTO **DEI** PRINCIPI FONDAMENTALI

LICEITÀ	
Quali sono le basi giuridiche che rendono il trattamento legittimo?	
Basi giuridiche Reg. UE 679/2016	**Finalità corrispondente**
Dati comuni	
☐ L'interessato ha espresso il **consenso** (art. 6.1-a) *	
☐ Il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6.1-b) *	
☐ Il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento	

(art. 6.1-c) *	
☐ Il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica (art. 6.1-d)	
☐ Il trattamento è 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 (art. 6.1-e)	
☐ il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi (art. 6.1-f) *	
Dati particolari	
☐ l'interessato ha prestato il proprio **consenso** esplicito al trattamento di tali dati personali per una o più finalità specifiche (art. 9.2-a) *	
☐ il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro** e della sicurezza sociale e protezione sociale (art. 9.2-b)	
☐ il trattamento è necessario per tutelare un **interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (art. 9.2-c)	
☐ il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una **fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle	

sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato (art. 9.2-d)	
☐ il trattamento riguarda dati personali resi **manifestamente pubblici** dall'interessato (art. 9.2-e)	
☐ il trattamento è necessario per accertare, esercitare o difendere **un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (art. 9.2-f)	
☐ il trattamento è necessario per motivi di **interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9.2-g)	
☐ il trattamento è necessario per finalità di **medicina preventiva o di medicina del lavoro**, valutazione della capacità lavorativa del dipendente, **diagnosi, assistenza o terapia sanitaria o sociale** ovvero **gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (art. 9.2-h)	
☐ il trattamento è necessario per motivi di **interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9.2-i)	
☐ il trattamento è necessario a fini di **archiviazione nel pubblico interesse**, di **ricerca scientifica o storica** o a fini	

statistici (art. 9.2-j)	
* Consenso	
* **Viene richiesto il consenso agli interessati?**	* DESCRIVERE COME VIENE RICHIESTO IL CONSENSO:
☐**SI** ☐**NO**	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

TRASPARENZA	
Viene fornita l'informativa agli interessati?	→ DESCRIVERE COME VIENE FORNITA L'INFORMATIVA AGLI INTERESSATI:
☐**SI** ☐**NO**	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

FINALITÀ	
Le finalità del trattamento sono esplicite, specifiche e legittime?	→ MOTIVARE LA RISPOSTA:
☐**SI** ☐**NO**	

VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE

MINIMIZZAZIONE	
I dati trattati sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati?	→ MOTIVARE LA RISPOSTA:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

PROPORZIONALITÀ	
Il Titolare può raggiungere la medesima finalità utilizzando meno dati personali, dati anonimi o dati pseudonimizzati?	→ MOTIVARE LA RISPOSTA:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

ESATTEZZA	
I dati sono accurati e mantenuti	→ DESCRIVERE IN CHE MODO:

aggiornati?	
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

LIMITAZIONE DELLA **CONS**ERVAZIONE		
Il trattamento dei dati avrà una durata non superiore a quella necessaria alle finalità per i quali i dati sono trattati?	**Finalità**	**Tempo di conservazione**
☐SI ☐NO		
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE		
→ PARERE DEL DPO:		

MISURE DI PROTEZIONE DEI DIRITTI DEGLI INTERESSATI

È stata adottata una procedura di gestione dei diritti degli interessati?	
☐ **SI**	→ ALLEGARE LA PROCEDURA (ALL. N. __)
☐ **NO**	→ INDICARE COME VENGONO RACCOLTE LE RICHIESTE DEGLI INTERESSATI:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

→ INDICARE COME VIENE GARANTITO IL DIRITTO DI ACCESSO:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:
✱ ✱ INDICARE COME VIENE GARANTITO IL DIRITTO ALLA PORTABILITÀ:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:
→ INDICARE COME VIENE GARANTITO IL DIRITTO DI RETTIFICA:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE

→ PARERE DEL DPO:
→ INDICARE COME VIENE GARANTITO IL DIRITTO ALLA CANCELLAZIONE:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:
→ INDICARE COME VIENE GARANTITO IL DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:
✱ INDICARE COME VIENE GARANTITO IL DIRITTO DI OPPOSIZIONE AL TRATTAMENTO:
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e formalizzati in un contratto?	→INDICARE LA PROCEDURA SEGUITA PER LA NOMINA A RESPONSABILE DEL TRATTAMENTO:
☐**SI** ☐**NO** ☐**Il trattamento non prevede il ricorso a responsabili**	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	

→ PARERE DEL DPO:

Prima della nomina a responsabile viene verificato che il fornitore presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate?	→ INDICARE LE MODALITÀ DI VERIFICA:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Gli obblighi degli autorizzati al trattamento sono chiaramente identificati e formalizzati in un contratto?	→ INDICARE LA PROCEDURA SEGUITA PER LA NOMINA DEGLI AUTORIZZATI AL TRATTAMENTO:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Gli autorizzati al trattamento sono stati adeguatamente formati per trattare correttamente i dati personali?	→ INDICARE LE SVOLGIMENTO DELLA FORMAZIONE E DI VERIFICA DI ACQUISIZIONE DELLE COMPETENZE:
☐SI	

☐NO ☐**Il trattamento non prevede il ricorso ad autorizzati**	

La formazione viene svolta con cadenza:

☐ semestrale

☐ annuale

☐ biennale

☐ altro (→ SPECIFICARE _____)

☐ non previsto

VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE

→ PARERE DEL DPO:

I dati vengono trasferiti al di fuori dell'Unione Europea?	→ INDICARE LE MISURE DI PROTEZIONE DEI DATI IN CASO DI TRASFERIMENTO:
☐**SI** ☐**NO**	

VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE

→ PARERE DEL DPO:

MISURE DI SICUREZZA ESISTENTI O PIANIFICATE

I documenti cartacei sono protetti?	→ INDICARE LE MODALITÀ DI PROTEZIONE DEI DOCUMENTI CARTACEI:
☐SI ☐NO ☐Il trattamento non avviene tramite documenti cartacei	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Le aree e i locali in cui si svolge il trattamento sono protetti?	→ INDICARE LE MODALITÀ DI PROTEZIONE DELLE AREE E DEI LOCALI:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Viene effettuato il backup dei dati?	→ INDICARE LA FREQUENZA CON CUI VENGONO SVOLTI I BACKUP:
☐SI ☐NO ☐ dati non sono conservati in un database elettronico	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Le postazioni di lavoro sono protette?	→ INDICARE LE MODALITÀ DI PROTEZIONE DELLE POSTAZIONI DI LAVORO:
☐ SI ☐ NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

Viene gestito il controllo dell'accesso logico?	→ INDICARE LE MODALITÀ DI GESTIONE DELL'ACCESSO LOGICO:
☐ SI ☐ NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	
→ PARERE DEL DPO:	

È stato stipulato un contratto di manutenzione software, hardware e gestione reti?
☐ SI ☐ NO
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE
→ PARERE DEL DPO:

I canali informativi sono protetti?	→ INDICARE LE MODALITÀ DI GESTIONE DELL'ACCESSO LOGICO:
☐ SI	

☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Viene garantita la protezione dai rischi non antropici?	→ INDICARE COME VENGONO GESTITI I RISCHI NON ANTROPICI:
☐SI ☐NO	
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

IMPATTI SUI DIRITTI DEGLI INTERESSATI E MISURE PER MITIGARE I RISCHI

ANALISI DEI RISCHI

SCALA DELLE PROBABILITÀ (P)

CRITERIO	LIVELLO	VALORE
- La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti - L'evento non si è mai verificato negli ultimi 5 anni - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe	IMPROBABILE	1

incredulità in azienda		
- La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi - L'evento si è verificato negli ultimi 5 anni e/o ci si aspetta una frequenza fra 1 e 3 anni - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una grande sorpresa in azienda	POCO PROBABILE	2
- La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto - L'evento si è verificato negli ultimi 3 anni e/o ci si aspetta una frequenza fra 1 mese ed 1 anno - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe una moderata sorpresa in azienda	PROBABILE	3
- Esiste una correlazione diretta tra la mancanza rilevata e il verificarsi del danno ipotizzato - L'evento si è verificato nell'ultimo mese e/o ci si aspetta una frequenza inferiore a 1 mese - Il verificarsi del danno conseguente la mancanza rilevata susciterebbe alcuno stupore in azienda	MOLTO PROBABILE	4

SCALA DELL'ENTITÀ DEL DANNO (GRAVITÀ) (G)

CRITERIO	LIVELLO	VALORE
- Episodio con effetti rapidamente reversibili per la struttura e gli strumenti in uso - Dati che potranno essere rapidamente ripristinati	LIEVE	1
- Episodio con effetti reversibili per la struttura e gli strumenti in uso - Dati che potranno essere certamente ripristinati entro 7 giorni	MEDIO	2
- Episodio con effetti difficilmente reversibili per la struttura e gli strumenti in uso - Dati che potranno difficilmente e/o solo in parte essere ripristinati entro 7	GRAVE	3

giorni		
- Episodio con effetti irreparabili per la struttura e gli strumenti in uso - Dati che non potranno essere ripristinati	GRAVISSIMO	4

MINACCE

Accesso non autorizzato **alle aree** ad accesso ristretto	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1)

	☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Sottrazione o danneggiamento di strumenti contenenti dati personali	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Poco probabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Poco grave 1 ☐ Poco grave 2 ☐ Grave 3 ☐ Gravissimo 4

Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Catastrofi **ambien**tali/Eventi distr**uttivi** d**o**losi	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Media 2 ☐ Grave 3

	☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Software malevoli	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2

	☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Spamming	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1

	☐ Minore 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Malfunzionamento, indisponibilità o degrado degli strumenti	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4

Stima della gravità (G)	☐ [illegible] ☐ [illegible] 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	**PxG=**
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Accessi non autorizzati a PC e reti informatiche	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ [illegible] 1 ☐ [illegible] 2 ☐ Probabile 3

	☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Intercettazione di informazioni in rete	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2

	☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Deterioramento dei supporti di memorizzazione	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1

	☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Sottrazioni delle credenziali di autenticazione	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	

Stima della probabilità del rischio (P)	☐ [illegible] 1 ☐ [illegible] 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ [illegible] 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Carenza di consapevolezza, disattenzione, incuria	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	

Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Poco probabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Lieve 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Comportamenti sleali o fraudolenti degli operatori	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	

Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE ➔ PARERE DEL DPO:	

Errori umani nella gestione della sicurezza fisica

Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mesi (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Utilizzo improprio di internet e della posta elettronica	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	[illegible] 1 [illegible] 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	[illegible] [illegible] ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	

Uso illegale dei software	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE	

→ PARERE DEL DPO:

Uso non autorizzato dei supporti di memorizzazione	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)

VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:

Uso di **software** da parte di **utenti non** autorizzati	
Quali impatti si verificherebbero sui soggetti interessati qualora il rischio si verificasse?	
Quali sono le principali vulnerabilità che possono condurre al rischio?	
Quali misure di sicurezza contribuiscono a gestire il rischio?	
Stima della probabilità del rischio (P)	☐ Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
Stima della gravità (G)	☐ Lieve 1 ☐ Medio 2 ☐ Grave 3 ☐ Gravissimo 4
Rischio residuo (R)	PxG=
Priorità degli interventi	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8)

	☐ immediata (9-16)
VALUTAZIONE: ☐ ACCETTABILE ☐ NON ACCETTABILE → PARERE DEL DPO:	