IMMEDIATAMENTE ESECUTIVA

AZIENDA OSPEDALIERA
OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO

DELIBERA DEL DIRETTORE GENERALE

N° 2104 **DEL** 22 DIC 2022

OGGETTO: Approvazione procedura: "*Elaborazione Data Protection Impact Assessment – DPIA - ovvero Valutazione di impatto sulla protezione dei dati*".

STRUTTURA PROPONENTE: U.O.C. COORDINAMENTO STRUTTURE DI STAFF **PROPOSTA N°** 317 **DEL** 20.12.2022

Il Dirigente e/o il responsabile del procedimento attestano – con la sottoscrizione del presente atto ed a seguito dell'istruttoria effettuata – la regolarità della procedura seguita, che l'atto è legittimo nella forma e nella sostanza nonché utile per il servizio pubblico.

L'ESTENSORE DEL PROVVEDIMENTO	IL RESPONSABILE DEL PROCEDIMENTO	IL DIRETTORE DELLA STRUTTURA PROPONENTE
Dr.ssa Emanuela Carbonaro	*Dr.ssa Emanuela Carbonaro*	*Dr. Tommaso Mannone*
(firma)	*(firma)*	*(firma)*
Data: 20.12.2022	Data: 20.12.2022	Data: 20.12.2022

Il Funzionario addetto al controllo di budget attesta – con la sottoscrizione del presente atto – che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico e, pertanto, ne attesta la copertura economica dei costi. Attesta, inoltre, il NULLA OSTA in quanto conforme alle norme sulla contabilità.

Conto Economico *(n°)*: /

Importo *(€)*: nessun onere

Sub-autorizzazione *(numero)*: /

IL FUNZIONARIO ADDETTO AL CONTROLLO DI BUDGET	Data	Firma
Dr. _____	21-12-2022	Il Direttore dell'U.O.S. Programmazione Pluriennale, Bilancio e Budget Dott.ssa Giuliana Alga

PARERE DEL DIRETTORE AMMINISTRATIVO Dr.ssa Loredana Di Salvo	PARERE DEL DIRETTORE SANITARIO Dr. Aroldo Gabriele Rizzo
☒ Favorevole ☐ Non Favorevole *(con motivazioni allegate al presente atto)*	☒ Favorevole ☐ Non Favorevole *(con motivazioni allegate al presente atto)*
Data 21/12/2022 Firma	Data 22/12/22 Firma

Il presente provvedimento si compone di n. ____ pagine, di cui n. ____ pagine di allegati.

IL DIRETTORE GENERALE
Dr. Walter Messina

In data 22 DIC 2022 nella sede legale dell'Azienda Ospedaliera "*Ospedali Riuniti Villa Sofia – Cervello*" di Palermo, Viale Strasburgo n. 233, P.I. 05841780827

IL DIRETTORE GENERALE

Dr. Walter Messina

nominato con Decreto Presidenziale n. 198 del 04/04/2019, con durata del rapporto contrattuale prorogato con deliberazione di Giunta Regionale n. 296 del 31/05/2022, con l'intervento del Direttore Amministrativo Dr.ssa Loredana Di Salvo, nominato con Delibera n. 101 del 26.01.2021 e del Direttore Sanitario Dr. Aroldo Gabriele Rizzo, nominato con Delibera n. 257 del 21.06.2019, assistito dal segretario verbalizzante Giuseppe Bartolotta, adotta la seguente deliberazione.

AZIENDA OSPEDALIERA
OSPEDALI RIUNITI VILLA SOFIA - CERVELLO PALERMO

DELIBERA DEL DIRETTORE GENERALE

U.O.C. Coordinamento Strutture di Staff
U.O.S Protezione dati personali
Dr.ssa Emanuela Carbonaro

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);

ATTESO che le norme introdotte dal Regolamento UE 2016/679 (GDPR) si traducono in adempimenti organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di protezione dati personali di cui al D. Lgs. 30.06.2003 n.196;

VISTO altresì il provvedimento n.580 del 21.4.2021 con cui è stato conferito incarico a tempo determinato di Dirigente Analista per le funzioni, tra l'altro, di Data Protection Officer (DPO) alla d.ssa Emanuela Carbonaro;

DATO ATTO che, con deliberazione n.656 del 3.10.2019, è stato costituito il Gruppo di Lavoro per la Protezione dei Dati;

DATO ATTO altresì che, con deliberazione n.657 del 3.10.2019, è stato costituito l'Ufficio per la Protezione dei Dati;

CONSIDERATO che questa Azienda, Titolare del trattamento dei dati personali, nella persona del rappresentante legale e Direttore Generale, ha aderito ai dettami del legislatore europeo mediante l'adozione dei provvedimenti sopra richiamati e avviando azioni di carattere organizzativo - gestionale nel rispetto di quanto disposto dal Regolamento UE 2016/679;

VISTI gli articoli 35 e 36 del Regolamento UE 2016/679 (GDPR) che disciplinano i casi in cui è obbligatorio effettuare la DPIA e la gestione dei rischi;

RITENUTO altresì di procedere all'approvazione della procedura: "*Elaborazione Data Protection Impact Assessment – DPIA - ovvero Valutazione di impatto sulla protezione dei dati*" e degli allegati al presente provvedimento quali parti integranti:

- ✓ Allegato 1: Elementi da considerare per la redazione DPIA

- ✓ Allegato2: Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto
- ✓ Allegato3: Metodologia utilizzata per l'analisi dei rischi

ATTESO che con la sottoscrizione del presente provvedimento si dichiara che l'istruttoria è corretta, completa e conforme alle risultanze degli atti d'ufficio;

ATTESO che il Responsabile del procedimento e il Responsabile della struttura proponente attestano inoltre, l'assenza di conflitto di interessi, ai sensi della normativa vigente e del Codice di Comportamento;

ATTESO che il Responsabile della Struttura proponente attesta la liceità e la regolarità delle procedure poste in essere con il presente provvedimento, in quanto legittime ai sensi della normativa vigente con riferimento alla materia trattata, nonché attesta l'utilità e l'opportunità per gli obiettivi aziendali e per l'interesse pubblico;

PROPONE

Per i motivi indicati in premessa che qui si intendono integralmente riportati, di:

1. approvare la procedura: "*Elaborazione Data Protection Impact Assessment – DPIA - ovvero Valutazione di impatto sulla protezione dei dati*" e gli allegati al presente provvedimento quali parti integranti:

- ✓ Allegato 1: Elementi da considerare per la redazione DPIA
- ✓ Allegato2: Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto
- ✓ Allegato3: Metodologia utilizzata per l'analisi dei rischi

2. dare atto che il presente provvedimento non comporta onere di spesa per l'Azienda;

3. incaricare le strutture competenti dell'esecuzione del presente provvedimento;

4. disporre l'immediata esecuzione della presente deliberazione, ai sensi del punto 7 dell'art. 53 della L. reg. n. 30/1993, al fine di consentire l'adozione della procedura di che trattasi con tempestività;

5. dare atto che la predetta procedura entrerà in vigore dal giorno successivo all'adozione del presente provvedimento;

6. notificare il presente provvedimento, a cura dell'Ufficio Protezione Dati, alla I.C.T. Management per provvedere alla pubblicazione sul sito web aziendale alla sezione

DELIBERA DEL DIRETTORE GENERALE

Protezione Dati https://ospedaliriunitipalermo.it/privacy_iconcina_laterale.html in ottemperanza degli obblighi di cui al D. Lgs. 33/2013 e affinché sia assicurata massima pubblicità e diffusione;

L'ESTENSORE
DEL PROVVEDIMENTO
Dr.ssa Emanuela Carbonaro

IL RESPONSABILE
DEL PROCEDIMENTO
Dr.ssa Emanuela Carbonaro

IL RESPONSABILE
DELLA STRUTTURA PROPONENTE
Dr. Tommaso Mannone

IL DIRETTORE GENERALE

IN VIRTÙ del Decreto del Presidente della Regione Siciliana n. 198 del 04 aprile 2019 di nomina del Dr. Walter Messina, quale Direttore Generale dell'Azienda Ospedaliera Ospedali Riuniti Villa Sofia Cervello;

VISTA la proposta di deliberazione che precede avente ad oggetto: "*Elaborazione Data Protection Impact Assessment – DPIA - ovvero Valutazione di impatto sulla protezione dei dati*"

ACQUISITI i pareri favorevoli espressi dal Direttore Amministrativo Aziendale e dal Direttore Sanitario Aziendale;

RITENUTO di condividerne il contenuto;

DELIBERA

Di adottare la proposta di deliberazione per come sopra formulata dal Responsabile della Struttura proponente e conseguentemente di:

DELIBERA DEL DIRETTORE GENERALE

1. approvare la procedura: "*Elaborazione Data Protection Impact Assessment – DPIA - ovvero Valutazione di impatto sulla protezione dei dati*" e gli allegati al presente provvedimento quali parti integranti:

- ✓ Allegato 1: Elementi da considerare per la redazione DPIA
- ✓ Allegato2: Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto
- ✓ Allegato3: Metodologia utilizzata per l'analisi dei rischi

2. dare atto che il presente provvedimento non comporta onere di spesa per l'Azienda;

3. incaricare le strutture competenti dell'esecuzione del presente provvedimento;

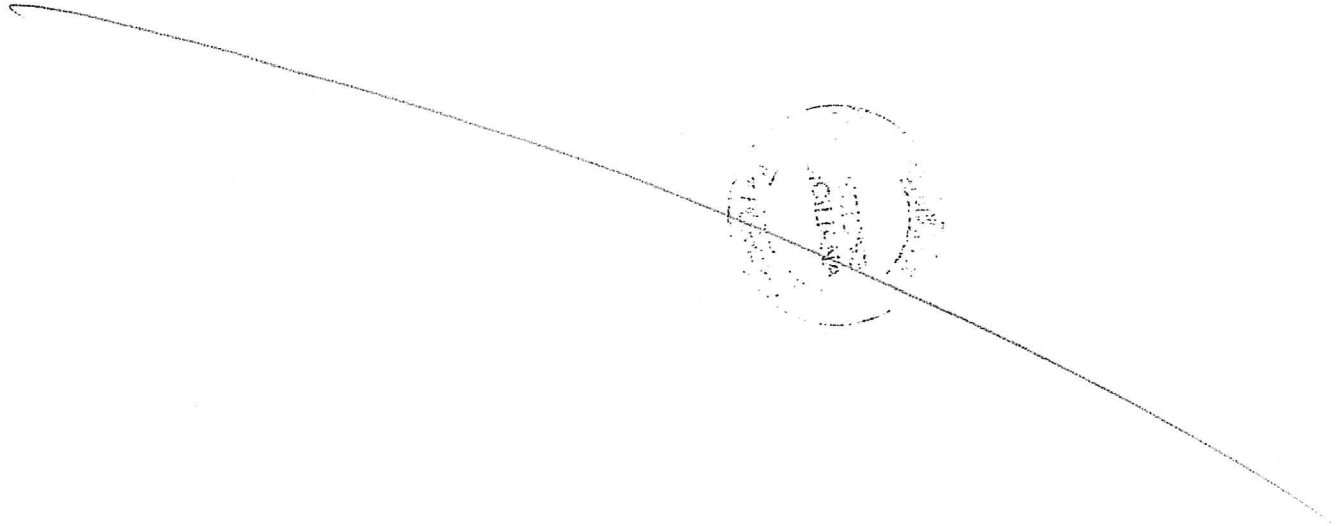
4. disporre l'immediata esecuzione della presente deliberazione, ai sensi del punto 7 dell'art. 53 della L. reg. n. 30/1993, al fine di consentire l'adozione della procedura di che trattasi con tempestività;

5. dare atto che la predetta procedura entrerà in vigore dal giorno successivo all'adozione del presente provvedimento;

6. notificare il presente provvedimento, a cura dell'Ufficio Protezione Dati, alla I.C.T. Management per provvedere alla pubblicazione sul sito web aziendale alla sezione Protezione Dati https://ospedaliriunitipalermo.it/privacy_iconcina_laterale.html in ottemperanza degli obblighi di cui al D. Lgs. 33/2013 e affinché sia assicurata massima pubblicità e diffusione.

IL DIRETTORE GENERALE
Dr. Walter Messina

Il segretario verbalizzante
Giuseppe Bartolotta



REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

PROCEDURA

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEL DATO - DPIA

Azienda Ospedaliera

"Ospedali Riuniti Villa Sofia - Cervello"

Palermo

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

Sommario

1. PREMESSA

Il Data Protection Impact Assessment (DPIA) o "Valutazione di impatto sulla protezione dei dati" è una delle fondamentali attività previste dal Regolamento UE 2016/679, relativamente agli obblighi dei Titolari art. 35 del RGPD, nell'ambito della gestione del rischio correlato al trattamento di dati personali.
La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per ridurli.

La valutazione d'impatto sulla protezione dei dati è uno strumento importante di responsabilizzazione in quanto sostiene il titolare del trattamento non soltanto nel rispettare i requisiti del Regolamento, ma anche nel dimostrare che sono state adottate misure appropriate.

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione oppure la mancata consultazione del Garante per la protezione dei dati personali laddove richiesto (articolo 36, paragrafo 3, lettera e), possono comportare sanzioni.

2. SCOPO E CAMPO DI APPLICAZIONE

Nell'ambito del contesto sopra descritto, il presente documento ha come obiettivo quello di fornire una guida metodologica, indicare attività e i compiti assegnati a diversi ruoli coinvolti nella valutazione dell'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento UE 2016/679, redatto in coerenza con l'approccio basato sul rischio previsto dalla normativa.

Verranno pertanto valutati i trattamenti posti in essere dall'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia – Cervello" di Palermo (d'ora in avanti "Azienda"), tracciati all'interno del "Registro delle attività di Trattamento", allorché, secondo l'art. 35 paragrafo 1 del RGPD, tali trattamenti prevedano in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità dei trattamenti "possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche", o ancora nel caso in cui ci si trovi di fronte di un nuovo trattamento che "può comportare un rischio elevalo per i diritti e le libertà delle persone fisiche".

Inoltre, ai sensi del sopracitato articolo, una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi o ancora.
Risulta pertanto fondamentale svolgere un'analisi preliminare per individuare tali trattamenti e dotarsi di principi e metodologie comuni per lo svolgimento delle attività di valutazione.

Al fine chiarire l'ambito e i confini di applicazione, le attività da eseguire e le responsabilità da coinvolgere, di seguito sarà illustrato il concetto di DPIA e sarà indicata la procedura da adottare nei casi in cui l'applicazione risulti obbligatoria.

3. RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito definito RGPD).
- 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, adottate il 4 aprile

2017 (versione successivamente emendata e adottata il 4 ottobre 2017) - WP 248 rev.01 – redatte dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI.

- Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali n. 467 dell'11 ottobre 2018 - *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* - 11 ottobre 2018 - *(Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018).*

4. DEFINIZIONI

Valutazione dell'impatto sulla protezione dei dati (DPIA): è la procedura prevista dall'articolo 35 del Regolamento UE 2016/679 che mira ad analizzare un trattamento di dati per valutarne la necessità e la proporzionalità, nonché i relativi rischi allo scopo di approntare misure idonee ad affrontarli.

RGPD: 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).

Rischio: è lo scenario descrittivo di un evento che agisce su un trattamento di dati e delle relative conseguenze che può comportare, che sono valutate in termini di gravità e probabilità di accadimento per i diritti e le libertà dei soggetti a cui i dati trattati si riferiscono.

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.

Registro delle attività di Trattamento: E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Sicurezza del trattamento: è costituita dall'insieme di elementi tecnici ed organizzativi correlati ad uno specifico trattamento e finalizzati a garantire disponibilità, integrità e riservatezza dei dati trattati.

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.

Violazione dei dati personali (*Personal Data Breach*): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

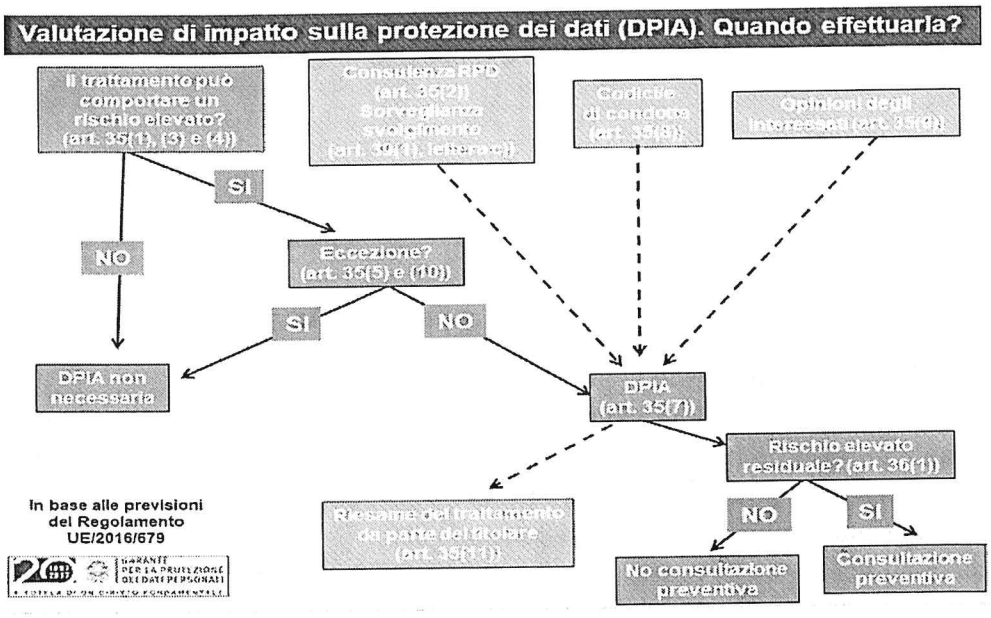
Responsabile per la Protezione dei Dati: è il soggetto individuato dal titolare ai sensi degli artt. 37-39 del RGPD, che ha compiti di controllo e di supporto all'organizzazione in tema di protezione dei dati personali. Di seguito può essere anche indicato con l'acronimo RPD o DPO.

Autorità di Controllo: Autorità Garante per la protezione dei dati personali.

WP29: Gruppo di lavoro composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'Unione Europea.

5. LE FASI DELLA VALUTAZIONE

Al fine di supportare i Titolari e i Responsabili nelle fasi di valutazione di impatto sulla protezione dei dati, il Garante per la Protezione dei Dati Personali ha realizzato efficacemente il seguente schema grafico, in coerenza con le linee guida appositamente redatte dal WP29:



Le fasi di processo per realizzare una DPIA sono più specificatamente dettagliate nel corso dei paragrafi seguenti.

6. ISTRUZIONI SUI CASI DI ATTUAZIONE DPIA

Una DPIA è un **processo** inteso ad analizzare un **trattamento di dati personali**, valutarne la necessità e la proporzionalità, nonché a contribuire a **gestire i rischi per i diritti e le libertà delle persone fisiche** derivanti dal trattamento stesso, **valutando detti rischi e** determinando **le misure per affrontarli**.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione, in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del RGPD, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del Regolamento. In altre parole, **una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità alla normativa in tema di protezione dei dati personali.**

Per una più puntuale descrizione dei criteri e dei trattamenti che devono essere oggetto di valutazione, si riporta all'**Allegato 2** del presente documento, l'***Elenco delle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto*** individuato dall'Autorità Garante per la Protezione dei Dati Personali con il provvedimento n. 467 dell'11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018).

Le Linee Guida WP 248 invitano ad **applicare la DPIA quando un trattamento soddisfi almeno due dei criteri precedentemente elencati**. In generale, il WP29 ritiene che maggiore sia 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 (fermo restando che il titolare stesso può decidere di condurre una DPIA anche se ricorre uno solo di tali criteri).

La DPIA dovrebbe essere condotta "prima di procedere al trattamento" (art. 35 paragrafi 1 e 10 del RGPD e considerando 93), impostazione anche coerente con i principi della privacy by design e by default (art. 25 del RGPD e considerando 78). La DPIA deve infatti essere considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento, sia prima del trattamento o anche in corso del trattamento, soprattutto quando esso risulta dinamico e soggetto a variazioni.

7. TRATTAMENTI NON SOGGETTI A DPIA

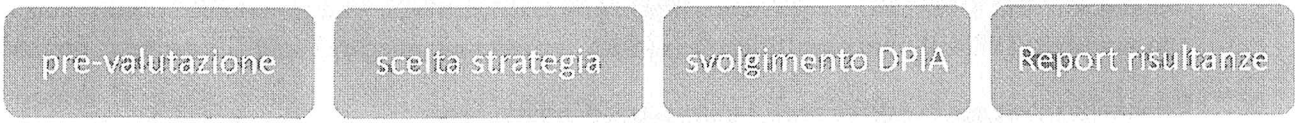
La DPIA non si applica nei seguenti casi:

- quando il trattamento non è tale da *"presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1)
- **quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati**. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35 paragrafo 119);
- qualora un trattamento sia effettuato ai sensi del **RGPD, articolo 6, paragrafo 1, lettera c)** (per obbligo legale al quale è soggetto il titolare del trattamento) **o lettera e)** (per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento) **e trovi nel diritto dell'Unione o nel diritto dello Stato membro** cui il titolare del trattamento è soggetto **una base giuridica** che disciplini il trattamento specifico o l'insieme di trattamenti in questione, o **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;
- **qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento** per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

Se valgono tali condizioni la DPIA non si applica (per cui non si applicano i paragrafi da 1 a 7 dell'art. 35 del RGPD), salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

8. PIANFICAZIONE DPIA

Per l'attività di pianificazione della DPIA, in modo da poter avere una visione globale e sistemica del processo, l'Azienda, procederà costituendo il gruppo di lavoro, condividendo gli obiettivi generali e di dettaglio e pianificando le attività come da processo grafico che segue:



Le fasi di lavoro prima indicate, verranno dettagliate nei paragrafi di seguito:

8.1 PRE-VALUTAZIONE

Il primo obiettivo dell'attività, a cura del Titolare del Trattamento con l'eventuale coinvolgimento delle figure preposte, riguarda la decisione circa l'opportunità di eseguire la DPIA su un trattamento di dati personali, rispetto ad un altro. Tale decisione è supportata da una rapida valutazione del rischio potenziale attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere dall'Azienda per la sua mitigazione e combinando i seguenti parametri, utili per tale identificazione:

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

Il Titolare del trattamento, valuta qualitativamente il danno e la probabilità connessi a ciascun trattamento sulla base dell'applicazione di specifiche scale di valutazione (allegato 3 – Metodologia utilizzata per l'analisi dei rischi).

E a seguito di questa prima analisi potremo ottenere 3 differenti tipologie di trattamento in base al rischio potenziale individuato:

1 Per tutti i trattamenti con potenziali di rischio non trascurabile sarà **OBBLIGATORIO** procedere con la DPIA come da indicazioni già fornite nel presente documento nel par. 5 "ISTRUZIONI SUI CASI DI ATTUAZIONE DPIA", anche ai sensi del provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione de dati personali (allegato 2 del presente documento);

2 Per tutti i trattamenti che soddisfano almeno due (2) dei criteri contenuti nel par. 5 "ISTRUZIONI SUI CASI DI ATTUAZIONE DPIA" e previsti dalle indicazioni del WP29 è **RACCOMANDATA** la DPIA per cui è sempre necessario procedere;
3 Per tutti i trattamenti che rappresentano un rischio trascurabile per i diritti e le libertà degli interessati, la DPIA **NON** sarà **NECESSARIA** (art. 35, paragrafo 1) come da indicazioni par. 7 del presente documento.

8.2 STRATEGIA GESTIONE DEL RISCHIO

Come input necessario allo svolgimento dell'attività di Valutazione d'Impatto e dopo aver concluso l'attività di pre-valutazione e individuati i trattamenti con alto potenziale di rischio e quelli per i quali è raccomandata la DPIA, sarà necessario definire ed individuare la strategia di gestione del rischio per i diritti e le libertà degli interessati, che dovrà essere utilizzata dal Titolare del Trattamento per lo svolgimento della DPIA. Tali asset dovranno essere formulati quali parte integrante della documentazione a corredo della DPIA al fine di giustificarne la scelta, per poter raggiungere i livelli di sicurezza prefissati.

Le possibili strategie da adottare per il trattamento del rischio sono:

1. condividere e mitigare i rischi con le parti interessate;

2. ridurre il rischio ad un livello ritenuto accettabile, attraverso l'implementazione delle contromisure necessarie al raggiungimento di tale soglia;

3. previa consultazione dell'autorità di controllo, accettare il rischio se non si ritiene opportuna nessuna delle precedenti opzioni;

Di seguito vedremo la gestione di ogni strategia prima proposta in conformità al Regolamento (UE) 2016/679.

8.2.1 CONDIVIDERE IL RISCHIO

Ogni qualvolta si è in presenza dell'utilizzo di nuove tecnologie che trattano dati personali, considerati la natura, l'oggetto, il contesto e le finalità dei trattamenti e approvvigionati da fornitori qualificati, sarà possibile condurre la DPIA per le attività di Trattamento, seguendo diverse modalità operative:

- ✓ Il fornitore nominato come Responsabile Esterno, dovrà fornire ogni informazione relativa documenti a supporto delle soluzioni tecnologiche adottate e certificazioni di conformità al RGPD o qualsiasi tipologia di certificazione di bene, servizio, processo o anche d'Azienda, che dimostrino la conformità agli standard di sicurezza e ai principi di privacy by design e privacy by default art. 25 del Regolamento UE 2016/679 che impone alle Aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali. Sulla base di tali certificazioni verrà condotta la DPIA;

- ✓ Il fornitore nominato come Responsabile Esterno, dovrà produrre un report di avvenuta "Valutazione d'Impatto" del bene o del servizio da fornire e sulla base di tale documento verrà

integrata e condotta la DPIA dell'Azienda Ospedaliera "Ospedali Riuniti Villa Sofia – Cervello" di Palermo;

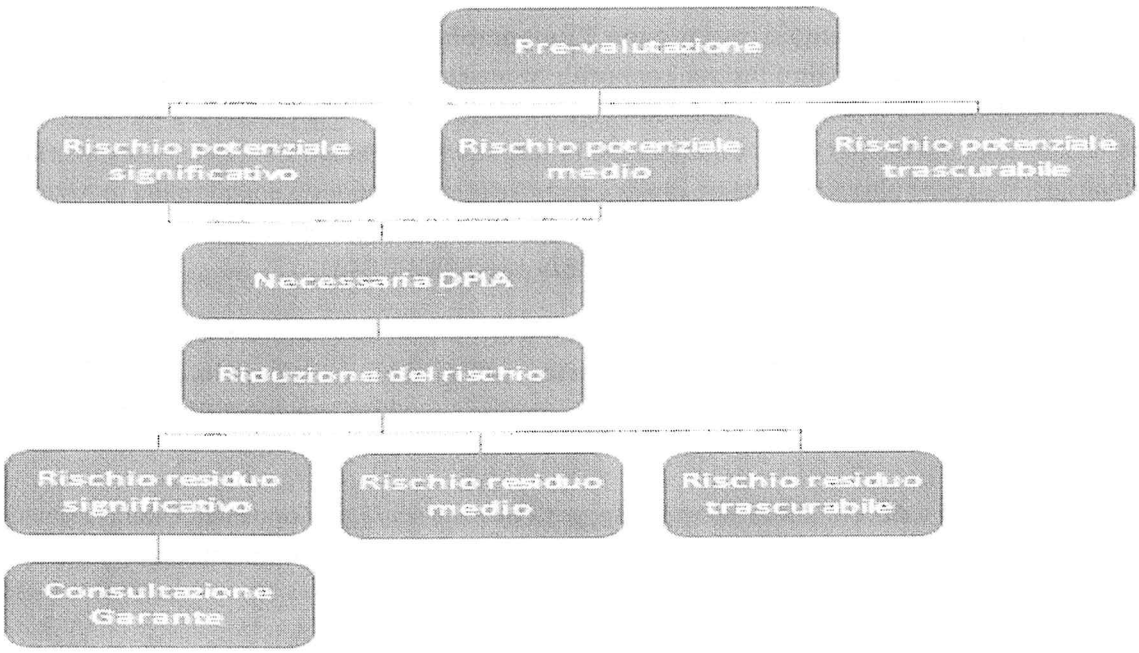
- ✓ In assenza delle opzioni precedenti, si potrà inoltrare al fornitore una check list da dover compilare. Con la scorta delle informazioni ottenute dalla check list si procederà con l'esecuzione della DPIA.

8.2.2 RIDURRE IL RISCHIO

Nel caso in cui si optasse per il trattamento di riduzione, il rischio di riferimento sarà quello ritenuto accettabile dal Titolare del Trattamento secondo le modalità operative dell'allegato 3 al presente documento, quale "Metodologia utilizzata per l'analisi dei rischi" e occorrerà valutare il livello di rischio residuo che si raggiungerà a valle della applicazione della strategia scelta ed i requisiti da attuare per il suo conseguimento, che saranno successivamente dettagliati all'interno di specifici report conclusivi.

A prescindere dal livello di rischio effettivo valutato, occorre definire una strategia di trattamento mirata a soddisfare tutti i requisiti normativi, non coperti o parzialmente coperti.

Possiamo comunque schematizzare l'intero iter di riduzione del rischio come di seguito:



8.2.3 CONSULTAZIONE PREVENTIVA AL GARANTE

Laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, per cui le misure adottate o pianificate non siano sufficienti per ridurre i rischi a un livello accettabile, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo

in relazione al trattamento (articolo 36, par. 1 e 3) giustificandone con appropriate informazioni, tale necessità.

Al momento di consultare l'autorità di controllo ai sensi dell'articolo 36 par. 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.

9. CHI EFFETTUA LA VALUTAZIONE

Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). La valutazione d'impatto sulla protezione dei dati può essere effettuata da altri soggetti, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito.

Inoltre il titolare del trattamento si consulta con il Responsabile della Protezione dei Dati (RPD), (articolo 35, paragrafo 2 RGPD) e con altre funzioni aziendali necessarie al processo di Valutazione come il Settore Tecnico e l'It Manager e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, devono essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il Responsabile della Protezione dei Dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)). Ulteriori orientamenti in merito sono forniti nelle *"Linee guida sui responsabili della protezione dei dati (RPD)"* del WP29 - 16/EN WP 243.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, **quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati** e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f)).

Il titolare può avvalersi della **collaborazione di soggetti esterni** per la redazione della valutazione d'impatto appositamente designati, come eventuali Responsabili Esterni o loro delegati, Consulenti Esterni.

10. ANALISI DELLA VALUTAZIONE

Nel rispetto delle disposizioni del Regolamento UE 2016/679, gli elementi volti a garantire la valutazione oggetto della procedura sono i seguenti:

1. descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

2. valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

3. valutazione dei rischi per i diritti e le libertà degli interessati di cui all'art. 35 paragrafo 1;

4. 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.

Si riporta di seguito lo schema di sintesi con le fasi di valutazione dell'analisi di impatto, con specifica della relativa della norma di riferimento e dei requisiti che ogni fase deve soddisfare:

Fase della valutazione DPIA	**Articolo RGPD di riferimento**	**Requisito**
Descrizione trattamento	art. 35, paragrafo 7, lettera a)	Descrizione dei seguenti punti: - Finalità del trattamento - Natura del trattamento - Ambito di applicazione - Contesto (normativo – organizzativo ecc.) - Dati personali registrati: - Destinatari del trattamento: - Periodo di conservazione dei dati personali - Descrizione funzionale del trattamento: - Individuazione delle risorse sulle quali sono registrati i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea); - Codici di condotta approvati applicabili (art. 35, paragrafo 8);
Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità	art. 35, paragrafo 7, lettera b)	Presenza di misure adeguate al fine di garantire: a) il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90) con riferimento a: - finalità specifiche, esplicite e legittime (art. 5(1), lettera b)); - liceità del trattamento (art. 6); - dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c)); - periodo limitato di conservazione (art. 5(1), lettera e)); b) la proporzionalità e la necessità del trattamento sulla base di: - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b)); - liceità del trattamento (articolo 6); - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c)); - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
Gestione dei rischi per i diritti e le libertà degli interessati	art. 35, paragrafo 7, lettera c)	a) Individuazione dei rischi in relazione alla loro: - origine, fonti, natura, particolarità e gravità (vedi considerando 84) con particolare riferimento a: accesso illegittimo, modifiche indesiderate, indisponibilità dei dati b) Individuazione dei diritti degli interessati e valutazione degli impatti potenziali su tali diritti e sulle libertà degli interessati stessi dei rischi descritti;

		c) individuazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati; d) stima delle probabilità e gravità (considerando 90); e) individuazione delle misure volte a gestire (eliminazione/mitigazione) i rischi di cui sopra (art. 35, paragrafo 7, lettera d) e considerando 90);
Coinvolgimento e parere degli interessati	art. 35, paragrafo 2 e 9	Il titolare chiede consulenza al RPD/DPO e, se del caso, provvede a coinvolgere gli interessati o i loro rappresentanti.

11. ELEMENTI VOLTI AD UNA EFFICACE VALUTAZIONE DEI RISCHI

Al fine di individuare correttamente i rischi e la loro gravità è necessario stimare gli aspetti relativi alla sicurezza del trattamento la cui compromissione può comportare almeno uno dei seguenti **danni per l'interessato**:

- Danno per la reputazione
- Discriminazione
- Furto di identità
- Perdite finanziarie
- Danni fisici o psicologici
- Perdita di controllo dei dati
- Altri svantaggi economici o sociali
- Impossibilità di esercitare diritti, servizi od opportunità.

Il Garante per la Protezione dei Dati Personali ha realizzato il seguente schema illustrativo relativo alle misure che è possibile adottare per la mitigazione del rischio:

12. OPINIONI DEGLI INTERESSATI

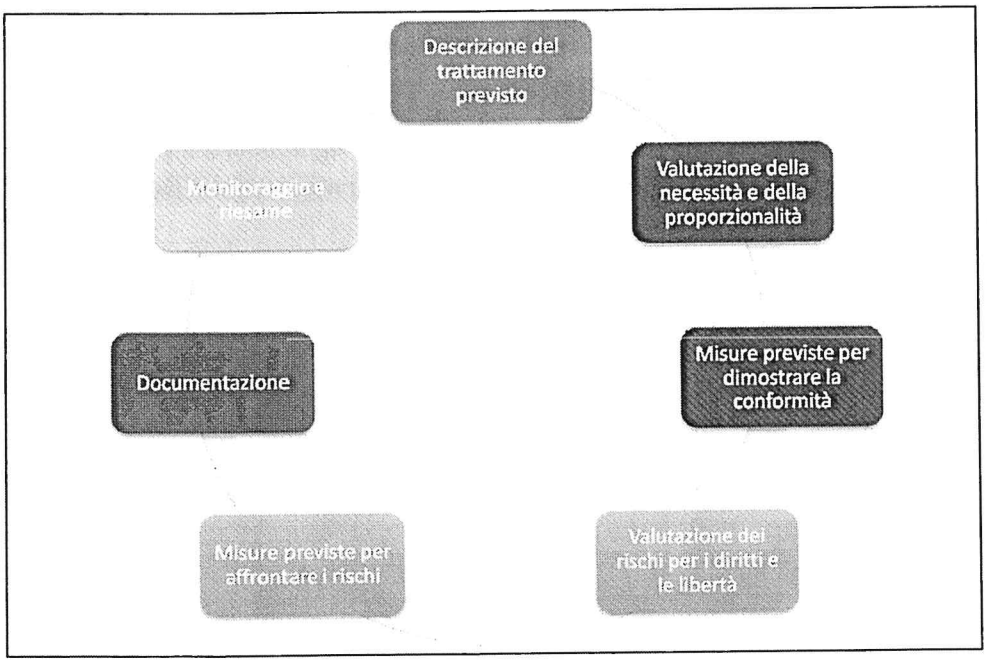
Il Titolare del Trattamento nella decisione sulla realizzazione e nello svolgimento della DPIA, se lo ritiene necessario, può anche acquisire il parere degli interessati o dei loro rappresentanti, come indicato dal Regolamento UE 2016/679 art. 35, par. 9 che cita, <<*se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto...*>>.

Il WP29 ritiene che:

- tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del titolare del trattamento), assicurando che il titolare del trattamento disponga di una base giuridica valida per il trattamento di qualsiasi dato personale interessato nel raccogliere dette opinioni (è opportuno osservare che il consenso al trattamento non è un modo idoneo per raccogliere le opinioni degli interessati);
- qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;
- il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò potrebbe comportare la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile.

13. MODALITÀ OPERATIVE PER LO SVOLGIMENTO DELLA DPIA

Il WP29, nelle Linee Guida WP 248 per la valutazione di impatto illustra il seguente processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati:



Al fine di effettuare una valutazione di impatto uniforme e confrontabile, è stata identificata una metodologia consolidata e diffusa, riportata in uno strumento che propone un percorso guidato coerente con il processo

illustrato nella figura precedente. La **CNIL**, (*Commission Nationale de l'Informatique et des Libertés* - Autorità francese per la protezione dei dati), ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA. La versione in lingua italiana è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

Al fine di semplificare l'applicazione di tale approccio metodologico, il redattore della DPIA potrà alternativamente redigere un documento testuale che compia un analogo percorso di valutazione. All'allegato 1 si riporta l'elenco degli elementi che devono essere presi in considerazione nella redazione del documento, qualora il soggetto titolato ritenga di redigere una DPIA senza ricorrere al software.

In merito alla modalità di valutazione del rischio, si riporta all'allegato 3 la metodologia proposta per l'analisi dei rischi, da utilizzare in caso di redazione della DPIA senza ricorso al software della CNIL.

14. ALLEGATI DEL PRESENTE DOCUMENTO

Si riportano di seguito gli allegati al presente documento, che ne costituiscono parte integrante:

Allegato 1 – Elementi da considerare per la redazione della DPIA;

Allegato 2 – Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto;

Allegato 3 – Metodologia utilizzata per l'analisi dei rischi.

15. REVISIONE DEL PRESENTE DOCUMENTO

Il documento sarà soggetto a modifiche ed aggiornamenti ogni qualvolta si renderà necessario. Tali aggiornamenti saranno approvati dal titolare del Trattamento, ma rilevati dal Responsabile per la Protezione dei Dati, che ne verificherà la rispondenza ai termini di legge.

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

ALLEGATO 1 – Elementi da considerare per la redazione della DPIA

Si riportano nell'elenco seguente gli elementi da inserire qualora si provveda alla redazione della DPIA senza ricorrere al software messo a disposizione dalla CNIL.

- **Informazioni sulla DPIA** (specificare denominazione, informazioni sull'autore, sul valutatore e sul validatore della DPIA)
- **Contesto**
  - Panoramica del trattamento (riportare le informazioni sul trattamento preso in considerazione, sulle responsabilità connesse, sugli standard applicabili)
  - Dati, processi e risorse di supporto (indicare i dati trattati, una descrizione funzionale del ciclo di vita dei dati, le risorse tecnologiche, cartacee, umane e di know-how impiegate nel trattamento)
- **Principi Fondamentali**
  - Proporzionalità e necessità (specificare se gli scopi del trattamento sono specifici, espliciti e legittimi, quali sono le basi legali che rendono lecito il trattamento, se i dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati, se i dati sono esatti e aggiornati e qual è il periodo di conservazione dei dati)
- **Misure a tutela dei diritti degli interessati** (Illustrare come gli interessati sono informati del trattamento, come eventualmente si ottiene il loro consenso, come eventualmente possono esercitare i loro diritti di accesso, portabilità, rettifica e cancellazione, limitazione ed opposizione; indicare se gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto e quali sono le misure di tutela adottate in caso di trasferimento dati al di fuori dell'Unione europea)
- **Rischi**
  - Misure esistenti o pianificate (illustrare le misure esistenti o pianificate per la mitigazione del rischio, quali ad esempio – a titolo esemplificativo e non esaustivo – crittografia, anonimizzazione, partizionamento, controllo degli accessi logici, tracciabilità applicata ai dati, ecc)
  - Metodo adottato per l'analisi dei rischi (indicare la metodologia applicata di analisi del rischio; per maggiori informazioni cfr. allegato 3)
  - Svolgimento dell'analisi dei rischi (indicare quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare e quali sono le principali minacce che potrebbero concretizzare il rischio; specificare quali sono le fonti di rischio e quali misure fra quelle individuate contribuiscono a mitigare il rischio; stimare la gravità e la probabilità di accadimento del rischio e il conseguente livello di esposizione al rischio sulla base del metodo di analisi dello stesso descritto precedentemente) per i 3 scenari seguenti:
  - Accesso illegittimo ai dati
  - Modifiche indesiderate dei dati
  - Perdita di dati
- **Piano d'azione** (illustrare gli interventi previsti nei seguenti contesti, specificati precedentemente nella DPIA)
  - Principi fondamentali
  - Misure esistenti e pianificate

- oRischi

➢ **Pareri**

- oParere DPO/RPD (indicare l'esito della verifica svolta dal DPO e il parere espresso)
- oParere degli interessati (specificare l'eventuale parere espresso dagli interessati o le motivazioni che hanno portato alla mancata richiesta)

15.1 ALLEGATO 2 – Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto

Si riporta di seguito l'elenco delle tipologie di trattamenti da sottoporre a valutazione di impatto, individuato dall'Autorità Garante per la Protezione dei Dati Personali con provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018), specificando quanto già riportato nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati WP 248 del GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI:

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

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

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-fitracking*) 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).

15.2 ALLEGATO 3 – Metodologia utilizzata per l'analisi dei rischi

Il modello scelto per valutare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
  - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
  - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
  - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

- Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).

- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
  - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	**Intervallo di valori**	**Intervento previsto**
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

1. REVISIONE DEL PRESENTE DOCUMENTO

Il documento sarà soggetto a modifiche ed aggiornamenti ogni qualvolta si renderà necessario. Tali aggiornamenti saranno approvati dal titolare del Trattamento, ma rilevati dal Responsabile per la Protezione dei Dati, che ne verificherà la rispondenza ai termini di legge.

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

ALLEGATO 2 – Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto

Si riporta di seguito l'elenco delle tipologie di trattamenti da sottoporre a valutazione di impatto, individuato dall'Autorità Garante per la Protezione dei Dati Personali con provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018), specificando quanto già riportato nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati WP 248 del GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI:

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).

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

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-fitracking*) 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.

15.1 ALLEGATO 3 – Metodologia utilizzata per l'analisi dei rischi

Il modello scelto per valutare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
  - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
  - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
  - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi,

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).
- Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).

- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
  - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	**Intervallo di valori**	**Intervento previsto**
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

1. REVISIONE DEL PRESENTE DOCUMENTO

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

Il documento sarà soggetto a modifiche ed aggiornamenti ogni qualvolta si renderà necessario. Tali aggiornamenti saranno approvati dal titolare del Trattamento, ma rilevati dal Responsabile per la Protezione dei Dati, che ne verificherà la rispondenza ai termini di legge.

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

ALLEGATO 3 – Metodologia utilizzata per l'analisi dei rischi

Il modello scelto per valutare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
  - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
  - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
  - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).
  - Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).
- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
  - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

REGIONE SICILIANA
Sede Legale Viale Strasburgo n.233 - 90146
Palermo
Tel 0917801111 - P.I. 05841780827

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	**Intervallo di valori**	**Intervento previsto**
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

AZIENDA OSPEDALIERA
OSPEDALI RIUNITI VILLA SOFIA CERVELLO PALERMO

DELIBERA DEL DIRETTORE GENERALE

PUBBLICAZIONE

Il sottoscritto dichiara che la presente deliberazione – ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n. 30/93 e dell'art. 32 della Legge n. 69/09 e s.m.i.– in copia conforme all'originale è stata pubblicata in formato digitale all'Albo on-line dell'Azienda Ospedaliera "*Ospedali Riuniti Villa Sofia – Cervello*", istituito sul sito www.ospedaliriunitipalermo.it, a decorrere dal giorno 25 DIC 2022 e che nei 15 giorni successivi:

☐ non sono pervenute opposizioni
☐ sono pervenute opposizioni da _____

L'ADDETTO
ALLA PUBBLICAZIONE

_____

IL FUNZIONARIO
INCARICATO

_____

Notificata al Collegio Sindacale il _____ prot. n. _____

DELIBERA NON SOGGETTA AL CONTROLLO

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4, comma 8, della L. n. 412/1991 e divenuta:

ESECUTIVA
decorso il termine (10 giorni dalla data di pubblicazione) ai sensi dell'art. 53, comma 6, L.R. n. 30/93

☐ Delibera non soggetta al controllo, ai sensi dell'art. 4, comma 8, della L. n. 412/1991 e divenuta:
IMMEDIATAMENTE ESECUTIVA
ai sensi dell'art. 53, comma 7, L.R. n. 30/93

IL FUNZIONARIO
INCARICATO

_____

ESTREMI RISCONTRO TURORIO

☐ Delibera trasmessa, ai sensi della L.R. 5/09, all'Assessorato Regionale Salute n. in data

_____

prot. n. _____

SI ATTESTA
che l'Assessorato Regionale Salute, esaminata la presente Deliberazione:

☐ ha pronunciato l'approvazione con atto prot. n. _____ del _____ come da allegato.

☐ ha pronunciato l'annullamento con atto prot. n. _____ del _____ come da allegato.

☐ Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n. 5/09 dal

_____

IL FUNZIONARIO
INCARICATO

_____

REGIONE SICILIA