REGIONE CALABRIA
GIUNTA REGIONALE

DIPARTIMENTO ORGANIZZAZIONE E RISORSE UMANE (ORU)
SETTORE 5 - DATORE DI LAVORO, SICUREZZA LUOGHI DI LAVORO, PRIVACY - RAPPORTI CON GLI ENTI LOCALI E POLIZIA LOCALE

Assunto il 13/10/2021

Numero Registro Dipartimento: 976

DECRETO DIRIGENZIALE

"Registro dei decreti dei Dirigenti della Regione Calabria"

N°. *10388 del 14/10/2021*

OGGETTO: APPROVAZIONE DEL PROCESSO DI GESTIONE DELLA PRIVACY BY DESIGN E BY DEFAULT PER LA REGIONE CALABRIA .

Dichiarazione di conformità della copia informatica

Il presente documento, ai sensi dell'art. 23-bis del CAD e successive modificazioni è copia conforme informatica del provvedimento originale in formato elettronico, firmato digitalmente, conservato in banca dati della Regione Calabria.

IL DIRIGENTE GENERALE

VISTI

- la Legge Regionale del 13 maggio 1996, n. 7 e s.m.i. recante “Norme sull’ordinamento della struttura organizzativa della Giunta Regionale e sulla Dirigenza Regionale”;

- la Delibera della G.R. 21/6/1999, n. 2661 recante “Adeguamento delle norme legislative e regolamentari in vigore per l’attuazione delle disposizioni recate dalla L.R. n. 7/96 e del D.Lgs. n. 29/93 e successive modifiche ed integrazioni”;

- il D.P.G.R. n. 354 del 24 giugno 1999 relativo alla Separazione dell’attività amministrativa di indirizzo e di controllo da quella gestionale, per come modificato ed integrato con il D.P.G.R. n. 206 del 5 dicembre 2000;

- la vigente struttura organizzativa della Giunta Regionale approvata con Delibera di Giunta Regionale n. 63 del 15.02.2019 e s.m.i. e R.R. n. 3 del 19.02.2019 e s.m.i., nonché la Delibera di Giunta Regionale n. 45 del 14.04.2020, con la quale è stato avviato l’iter di riorganizzazione delle strutture amministrative;

- la D.G.R. n. 91 del 15 maggio 2020 avente ad oggetto “Struttura organizzativa della Giunta Regionale – approvazione modifiche alla Deliberazione di G.R. n. 63 del 15.02.2019 e ss.mm.ii.”;

- la D.G.R. n. 237 del 7 agosto 2020 avente ad oggetto “Misure volte a garantire maggiore efficienza alla struttura organizzativa della Giunta Regionale -Approvazione modifiche ed integrazioni del Regolamento Regionale n. 3/2019 e s.m.i.”;

- la Deliberazione di Giunta Regionale n. 512 del 31.10.2019 riguardante l’assegnazione dei Dirigenti Regionali;

- lL D.D.G. 13992 del 18.12.2020 avente per oggetto: “Approvazione nuova struttura organizzativa del dipartimento "Organizzazione e Risorse Umane".

- il D.P.G.R. n. 17 del 24 febbraio 2021 con il quale è stato conferito all’Avv. Sergio Nicola Tassone l’incarico di Dirigente Generale Reggente del Dipartimento “Organizzazione e Risorse Umane” della Giunta Regionale;

- il D.D.G. n. 14101 del 15.11.2019, con il quale al Dott. Salvatore Lopresti è stato conferito l'incarico di Dirigente Settore Datore di Lavoro, privacy rapporti con gli enti locali e polizia locale del Dipartimento Organizzazione e Risorse Umane;

- il D.D.G. n. 3289 del 30.03.2021, con il quale, alla Dott.ssa Luigina Sgrizzi è stata assegnata la P.O. di 3^ fascia denominata “Privacy – Protezione dati” presso lo scrivente Settore;

- il decreto legislativo 30 marzo 2001, n. 165;

VISTI ALTRESI’

- il Regolamento (UE) 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 genera-

le sulla protezione dei dati" (di seguito "GDPR"), il decreto legislativo 30 giugno 2003, n.196 - "Codice in materia di protezione dei dati personali" adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018 n.101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio;

- l'articolo 8 della Convenzione Europea dei Diritti dell'Uomo del 1950 (CEDU) e l'articolo 16 del TFUE (Trattato sul funzionamento dell'Unione europea);

- la nota prot. SIAR n. 423736 del 4/10/2021 con la quale il Responsabile della Protezione Dati Regionale ha trasmesso il processo di gestione della privacy by design e by default per come elaborato nell'ambito del Progetto Identità Digitali e Sicurezza Servizi di Cloud Computing, di sicurezza, di realizzazione dei portali e servizi online e di cooperazione applicativa per le pubbliche amministrazioni – LOTTO 2 - elaborato da Leonardo S.p.a., in qualità di società mandataria del RTI composto da IBM Italia S.p.a., Sistemi Informativi S.r.l., Fastweb S.p.a ;

- la Delibera di Giunta Regionale n. 29 del 1 febbraio 2021 avente per oggetto: "Competenze in materia di trattamento dei dati personali – approvazione modifiche del Regolamento Regionale n. 20 del 18 dicembre 2018";

- il Regolamento regionale 18 dicembre 2018, n. 20, recante: "Attribuzione delle competenze in materia di trattamento dei dati personali nell'ambito delle strutture organizzative della Giunta Regionale" per come modificato dalla DGR 29/2021;

PRESO ATTO del documento "processo di gestione della privacy by design e by default" del 4/10/2021, redatto dalla società NTT DATA Italia S.p.A., in esecuzione dei servizi professionali previsti dal contratto esecutivo del 05/12/2019 CIG 8025774638, stipulato nell'ambito del contratto quadro Consip "SPC Cloud Lotto 2";

RICHIAMATA la deliberazione di Giunta regionale n. 11 del 28 gennaio 2021 con la quale l'esecutivo ha approvato il Piano Triennale della Prevenzione, della Corruzione e della Trasparenza 2021/2023 – Aggiornamento 2021;

RILEVATO CHE, in seguito alla approvazione della DGR n.29 del 1 febbraio 2021 è necessario adottare il processo di gestione della privacy by design e by default come elaborato nell'ambito del "Progetto Identità digitali e Sicurezza" e proposto dal Responsabile della Protezione Dati Regionale con nota prot. SIAR n.423736 del 4/10/2021;

CONSIDERATO CHE il regolamento regionale n. 20/2018 modificato dalla DGR 29/2021 definisce ruoli e competenze anche con riferimento alle modalità di gestione dei diritti degli interessati;

ACCERTATO CHE le modalità operative indicate nel processo di gestione della privacy by design e by default risultano coerenti con la ripartizione di ruoli e competenze previste nel citato Regolamento n.20 del 2018 per come modificato dalla DGR n.29 del 2021 nonché con le indicazioni fornite dal Garante per la Protezione dei Dati Personali;

VISTI altresì

- il Regolamento Europeo 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

-il Dlgs. n. 33/2013 e s.m.i;

DECRETA

per le motivazioni espresse in parte motiva e che qui si intendono integralmente riportate

1. DI APPROVARE il processo di gestione della privacy by design e by default per la Regione Calabria che allegato al presente provvedimento, insieme al diagramma di flusso, ne forma parte integrante e sostanziale;

2. DI DEMANDARE al Tavolo Tecnico istituito con DGR 29/2021, al Responsabile della Protezione Dati ed al Settore Datore di Lavoro e Privacy la divulgazione dei contenuti del processo a tutti i Delegati del Titolare per come individuati dall'art.1 comma 1 del Regolamento n.20 del 2018 per come modificato dalla DGR n.29 del 2021;

3. DI NOTIFICARE a cura del Dipartimento Organizzazione e Risorse Umane il presente provvedimento al Responsabile della Protezione Dati e a tutti i Dipartimenti e strutture equiparate della Giunta Regionale**;**

4. DI DISPORRE la pubblicazione integrale del presente provvedimento sul Bollettino Ufficiale della Regione Calabria ai sensi della Legge regionale 6 aprile 2011, n. 11, nonché la pubblicazione sul sito istituzionale della Regione Calabria ai sensi del D.Lgs. 14 marzo 2013, n. 33 e nel rispetto delle disposizioni di cui al D.lgs. 30 giugno 2003, n. 196 e s.m.i..

Sottoscritta dal Responsabile del Procedimento
SGRIZZI LUIGINA
(con firma digitale)

Sottoscritta dal Dirigente
LOPRESTI SALVATORE
(con firma digitale)

Sottoscritta dal Dirigente Generale
TASSONE SERGIO NICOLA
(con firma digitale)

Identificativo: D01_SCO.1_FASE1 Rev. 2.0

Data: 04/10/2021

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

CIG 8025774638

Regione Calabria

Processo di Privacy by design e by default

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo Divisione Cyber Security SpA

IBM SpA

Sistemi Informativi SpA

Fastweb SpA

	Nome e Ruolo	Firma
Autore di riferimento		
Verifica		
Approvazione		
Autorizzazione		

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autore di rif.
1.0	11/11/2020	Versione definitiva	
2.0	04/10/2021	Aggiornamento Processo e strumento Excel a supporto post DGR n. 29 del 01/02/2021	

Calendario degli Incontri Principali

Data	Incontro	Stato
10/02/2020	Approfondimento con Responsabile della Protezione dei Dati su ruoli, responsabilità e attività di gestione della privacy in Regione Calabria	Effettuato
24/02/2020	Intervista GDPR con DIPARTIMENTO ORGANIZZAZIONE, RISORSE UMANE	Effettuato
26/02/2020	Intervista GDPR con DIPARTIMENTO BILANCIO, FINANZE E PATRIMONIO	Effettuato
26/02/2020	Intervista GDPR con STAZIONE UNI<CA APPALTANTE	Effettuato
27/02/2020	Intervista GDPR con DIPARTIMENTO PRESIDENZA	Effettuato
27/02/2020	Intervista GDPR con DIPARTIMENTO ISTRUZIONE E ATTIVITA' CULTURALI	Effettuato
02/03/2020	Intervista GDPR con DIPARTIMENTO AMBIENTE E TERRITORIO	Effettuato
02/03/2020	Intervista GDPR con DIPARTIMENTO SEGRETARIATO GENERALE	Effettuato
03/03/2020	Intervista GDPR con DIPARTIMENTO INFRASTRUTTURE, LAVORI PUBBLICI E MOBILITA'	Effettuato
30/03/2020	Intervista GDPR con DIPARTIMENTO LAVORO, FORMAZIONE E POLITICHE SOCIALI	Effettuato
02/04/2020	Intervista GDPR con AUTORITA' DI AUDIT	Effettuato
03/04/2020	Intervista GDPR con DIPARTIMENTO TURISMO E SPETTACOLO	Effettuato
08/04/2020	Intervista GDPR con DIPARTIMENTO SVILUPPO ECONOMICO E ATTIVITA' PRODUTTIVE	Effettuato

Data	Incontro	Stato
08/04/2020	Intervista GDPR con DIPARTIMENTO PROGRAMMAZIONE NAZIONALE	Effettuato
09/04/2020	Intervista GDPR con DIPARTIMENTO AGRICOLTURA E RISORSE AGROALIMENTARI	Effettuato
14/04/2020	Intervista GDPR con DIPARTIMENTO TUTELA DELLA SALUTE E POLITICHE SANITARIE	Effettuato
15/04/2020	Intervista GDPR con DIPARTIMENTO PROGRAMMAZIONE COMUNITARIA	Effettuato
20/04/2020	Intervista GDPR con AVVOCATURA REGIONALE	Effettuato
27/04/2020	Intervista GDPR con NUCLEO VALUTAZIONE	Effettuato
08/05/2020	Intervista GDPR con DIPARTIMENTO URBANISTICA E BENI CULTURALI	Effettuato
14/05/2020	Intervista GDPR con ANTICORRUZIONE E TRASPARENZA	Effettuato
20/04/2021	Tavolo di coordinamento interdipartimentale protezione dati del 20 aprile 2021	Effettuato
27/05/2021	Tavolo di coordinamento interdipartimentale protezione dati del 27 maggio 2021	Effettuato
21/07/2021	Tavolo di coordinamento interdipartimentale protezione dati del 21 luglio 2021	Effettuato
24/09/2021	Tavolo di coordinamento interdipartimentale protezione dati del 24 settembre 2021	Effettuato

SOMMARIO

LISTA DELLE TABELLE

LISTA DELLE FIGURE

1 INTRODUZIONE

Il *Processo* descritto nel presente documento è rivolto sia al personale dipendente dell'Amministrazione regionale sia al personale non dipendente che collabora con l'Ente tra cui in particolare ai soggetti proponenti di nuove iniziative progettuali, che comportano il trattamento di dati personali di titolarità dell'Ente, o di nuovi trattamenti nell'ambito di iniziative già avviate.

Gli obiettivi del suddetto *Processo*, eseguito ogniqualvolta si intenda avviare o modificare significativamente una iniziativa/trattamento, sono sanciti dall'art. 25 del GDPR e riguardano la "protezione dei dati fin dalla progettazione" (*Data Protection by Design*) e la "protezione per impostazione predefinita" (*Data Protection by Default*).

La *Data Protection by Design* è stabilita dal par. 1 dell'art. 25:

"[…] sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati […]".

La *Data Protection by Design* prevede inoltre che le misure da mettere in atto tengano conto dello stato dell'arte, dei costi di attuazione, del contesto, delle finalità del trattamento e dei rischi per i diritti e le libertà degli interessati.

La *Data Protection by Default* è stabilita invece dal par. 2 dell'art. 25:

"*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento […]*"

La *Data Protection by Default* prevede inoltre che il trattamento avvenga per il solo periodo strettamente necessario al raggiungimento delle finalità previste e che i dati non siano accessibili ad un numero indefinito di persone.

Il perseguimento degli obiettivi di *Data Protection by Design e by Default* comporta un'attività continua, lungo tutto il ciclo di vita dell'iniziativa progettuale, di valutazione e integrazione delle misure di protezione più adeguate da applicare, cominciando già dalla primissima fase di progettazione e continuando fino al termine di tutti i trattamenti di dati personali in corso.

Per ogni nuova iniziativa proposta, occorre:

- esaminare attentamente il contesto e approfondire gli obiettivi dell'iniziativa, in modo da selezionare i dati personali effettivamente necessari;
- identificare i possibili scenari di rischio che si potranno verificare, per mettere da subito in campo le misure preventive più efficaci e ridurre al minimo gli interventi correttivi successivi;
- aggiornare costantemente le proprie competenze sulle misure di protezione disponibili, per sfruttarle opportunamente nel disegno di nuove iniziative, e/o anche, se occorre, adattando l'iniziativa stessa a tali vincoli di protezione;
- progettare soluzioni implementative trasparenti, che consentano di verificare facilmente i processi di trattamento dei dati personali e le relative misure di protezione.

Il GDPR non prescrive procedure o metodologie specifiche da rispettare, ma introduce chiari principi da applicare e obiettivi da raggiungere. È stato pertanto definito un *Processo di Privacy by design e by default* commisurato alle caratteristiche dell'Ente, tenendo conto delle politiche già in uso e garantendo un buon

bilanciamento tra aderenza alle best practice di riferimento, efficacia nel raggiungere gli obiettivi e facilità di applicazione. È stato inoltre realizzato uno strumento Excel a supporto delle attività previste, si veda l'Allegato 1, denominato "Privacy & Security Pre-Assessment (PSP)".

L'esecuzione di tale *Processo*, oltre al coinvolgimento primario:

- del *Soggetto Proponente* (che propone l'iniziativa),
- del *Settore referente privacy regionale* (che identifica gli interventi di sicurezza organizzativa e sicurezza fisica),
- del *Settore referente per la sicurezza informatica regionale* (che identifica gli interventi di sicurezza informatica) e
- del *Team implementativo* (che implementa i requisiti degli interventi da attuare),

può richiedere il contributo di ulteriori strutture organizzative interne e/o esterne, in relazione alla tipologia di requisiti e alle relative soluzioni da mettere in campo.

Il *Processo di Privacy by design e by default* qui definito concorre a dimostrare (cfr. "Accountability") la compliance all'art. 25 del GDPR. Al fine di garantire la continua aderenza al quadro normativo vigente, ai nuovi orientamenti strategici, alle modifiche relative all'attività, alla struttura organizzativa e di governance dell'Ente, il presente *Processo* sarà periodicamente riesaminato ed eventualmente modificato.

2 RIFERIMENTI

2.1 Documenti Applicabili

Rif.	Codice	Titolo
DA-1.	PRO_ITAL_170635 Rev. 4.1	Progetto dei fabbisogni
DA-2.	CIG 8025774638	Contratto Esecutivo del 05/12/2019

Tabella 1 Documenti applicabili

2.2 Documenti di Riferimento

Rif.	Codice	Titolo
DR-1.	WP248	Linee guida dello European Data Protection Board in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679.
DR-2.	MAN_ENISA	Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali.
DR-3.	AGID-MM	Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (circolare AgID n. 2/2017 del 18 aprile 2017)
DR-4.	DGR 29/2021	Regione Calabria, DGR n. 29 del 01/02/2021, Competenze in materia di trattamento dei dati personali - approvazione modifiche al regolamento regionale n.20 del 18 dicembre 2018
DR-5.	DD 6786/2021	Regione Calabria, DD n. 6786 del 30/06/2021, Metodologia di valutazione d'impatto per la protezione dei dati personali (DPIA)

Tabella 2 Documenti di riferimento

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Termine	Descrizione
Accountability	Ex art. 5, paragrafo 2 del GDPR: "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Il paragrafo 1 dell'art. 5 del GDPR riguarda i principi fondamentali che devono essere accuratamente applicati ai trattamenti di dati personali.
Misure di sicurezza	Misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.
DPIA	Data Protection Impact Assessment (o Privacy Impact Assessment): è la valutazione d'impatto sulla protezione dei dati. Tale processo è volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Lo stesso può riguardare una singola operazione di trattamento dei dati, ma potrebbe riferirsi anche a trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.

Tabella 3 Definizioni

3.2 Acronimi

Termine	Descrizione
GDPR	Regolamento generale (UE) 2016/679 sulla protezione dei dati
RPD/DPO	Responsabile della Protezione dei Dati Personali / Data Protection Officer
AGID	Agenzia per l'Italia Digitale
TRADES	Piattaforma applicativa regionale Trattamento Dati e Sicurezza
SRPR	Settore referente privacy regionale
SRSIR	Settore referente per la sicurezza informatica regionale

Tabella 4 Acronimi

4 RIFERIMENTI NORMATIVI

4.1 L'art. 25 del GDPR

Il principio della protezione dei dati personali "by design" afferma che i dati delle persone fisiche devono essere considerati e tutelati fin dalla fase di progettazione di qualsiasi iniziativa che ne preveda il trattamento, sia essa un processo, un sistema informatico, una tecnologia, etc. Il principio della protezione dei dati "by default" stabilisce invece che, per impostazione predefinita, i dati personali da trattare devono essere solo quelli necessari e sufficienti per le finalità previste e devono essere trattati per il solo periodo strettamente necessario a raggiungere tali finalità.

Tali principi sono introdotti dall'art. 25 del GDPR dal titolo "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".

Il paragrafo 1 dell'art. 25 stabilisce che il Titolare del trattamento dei dati personali deve adottare delle misure tecniche e organizzative al fine di dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati, garantendo in questo modo i diritti degli interessati. La norma prevede infatti che: *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati"*.

La predisposizione delle misure necessarie è prescritta sia nel momento in cui il Titolare del trattamento deve determinare i mezzi del trattamento stesso, sia quando egli pone in essere le vere e proprie operazioni di trattamento. Il Titolare, nell'attuare le misure previste, dovrà sempre tenere conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei diversi rischi per i diritti e le libertà degli interessati.

Il paragrafo 2 dell'art. 25 introduce la necessità che la protezione dei dati personali sia garantita "per impostazione predefinita" (by default). Il Regolamento stabilisce infatti che: "*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

Le valutazioni e gli interventi, relativi alle misure tecniche e organizzative da adottare, devono essere compiuti prima che i trattamenti vengano concretamente avviati e devono essere documentati.

4.2 Responsabilità

L'applicazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'art. 25 del GDPR, deve essere realizzata dal Titolare del trattamento, le cui responsabilità generali sono sancite dall'art. 24 del GDPR. Il par. 1 dell'art. 24 prescrive in particolare che "*[…] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*".

Il combinato disposto degli artt. 24, 25 e 32 ("Sicurezza del trattamento") del GDPR esplicita inoltre la necessità che le misure tecniche e organizzative adottate dal Titolare risultino adeguate rispetto ai rischi rilevati. Per garantire tale obiettivo, l'intera organizzazione privacy interna dovrà contribuire al processo di attuazione di tali misure seguendo un approccio orientato alla valutazione dei rischi.

4.3 Sanzioni

In caso di violazione o mancato adeguamento al GDPR, i tre criteri chiave per valutare l'applicabilità delle sanzioni sono: effettività, proporzionalità e dissuasività. Le sanzioni sono disciplinate dagli artt. 83 e 84 del GDPR.

Il par. 2 dell'art. 83 ("Condizioni generali per infliggere sanzioni amministrative pecuniarie") afferma, in particolare, che l'Autorità di controllo, al momento di decidere se infliggere o meno una sanzione amministrativa pecuniaria e di fissarne l'ammontare, dovrà ponderare la decisione considerando una serie di elementi, tra cui "*il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32*".

L'art. 25 è inoltre esplicitamente citato anche nel par. 4 (dell'art. 83) che stabilisce i criteri per quantificare le sanzioni amministrative pecuniarie.

L'art. 84 del GDPR, infine, prevede che siano gli Stati membri a stabilire le norme sulle altre sanzioni previste in caso di violazioni non sottoposte a misure di carattere amministrativo e pecuniario. Nel caso dell'Italia si fa riferimento al Codice della Privacy (decreto legislativo 30 giugno 2003, n. 196 e ss. mm. e ii.).

5 PROCESSO DI PRIVACY BY DESIGN E BY DEFAULT

5.1 Descrizione generale del Processo

Il *Processo di Privacy by design e by default*, rappresentato dal diagramma di Figura 1 riportato a seguire, stabilisce le attività da eseguire e i relativi attori coinvolti, allorquando si intenda avviare[1] una nuova iniziativa progettuale, che comporta il trattamento di dati personali di titolarità dell'Ente, o un nuovo trattamento nell'ambito di un'iniziativa già avviata.

Il *Processo* ha l'obiettivo di approfondire le caratteristiche principali dell'iniziativa proposta, di valutarne le criticità rispetto al trattamento dei dati personali e di determinare e mettere in campo gli interventi necessari per garantire un adeguato livello di sicurezza.

Le attività previste sono organizzate in tre fasi:

- *Fase 1: Analisi Iniziativa* - Analisi delle caratteristiche principali dell'iniziativa proposta e valutazione del relativo livello generale di criticità (standard/superiore) riguardo al trattamento dei dati personali;
- *Fase 2: Identificazione Interventi da Attuare* - Selezione dei provvedimenti e delle misure da adottare o consolidare a tutela dell'iniziativa proposta e verifica della loro fattibilità;
- *Fase 3: Monitoraggio Implementazione* - Monitoraggio dello stato di avanzamento delle attività di implementazione dei requisiti e gestione di eventuali proposte di soluzioni alternative.

Gli attori principali del *Processo* consistono in figure/team/strutture che detengono ruoli di responsabilità e direzione nelle suddette fasi. Per le attività più operative potranno essere coinvolte, in relazione alla specifica iniziativa in esame, anche ulteriori strutture organizzative interne e/o esterne.

Gli attori principali sono:

- *Proponente* - Figura professionale, team o struttura che propone nuove iniziative progettuali, che comportano il trattamento di dati personali di titolarità dell'Ente, o nuovi trattamenti nell'ambito di iniziative già avviate;
- *Settore referente privacy regionale* - Struttura responsabile del Processo, coinvolta nelle attività di identificazione degli interventi di sicurezza organizzativa e sicurezza fisica da attuare;
- *Settore referente per la sicurezza informatica regionale* - Struttura coinvolta nelle attività di identificazione degli interventi di sicurezza informatica da attuare;
- *Team implementativo* - Team coinvolto nel sotto processo di implementazione dei requisiti di sicurezza e privacy selezionati, composto da una o più strutture interne e/o esterne, in relazione alla tipologia di requisiti e alle relative soluzioni da mettere in campo.

L'esecuzione del *Processo di Privacy by design e by default* è supportata dallo strumento Excel "*Privacy & Security Pre-Assessment (PSP)*" descritto nell'Allegato 1. Tale strumento consente di valutare agevolmente l'iniziativa proposta e selezionare la Baseline[2] degli interventi, al netto di eventuali requisiti supplementari, raccomandati dal Processo di DPIA, condotto separatamente attraverso la piattaforma applicativa regionale TRADES[3] e la metodologia[4] di valutazione d'impatto per la protezione dei dati personali (DPIA) basata sul tool ARIEC.

1 Avviare una nuova iniziativa o anche "modificare significativamente" una iniziativa già avviata
2 Baseline degli interventi: requisiti minimi di privacy e sicurezza da implementare
3 Cfr. https://trades.regione.calabria.it
4 Cfr. decreto dirigenziale n. 6786 del 30/06/2021

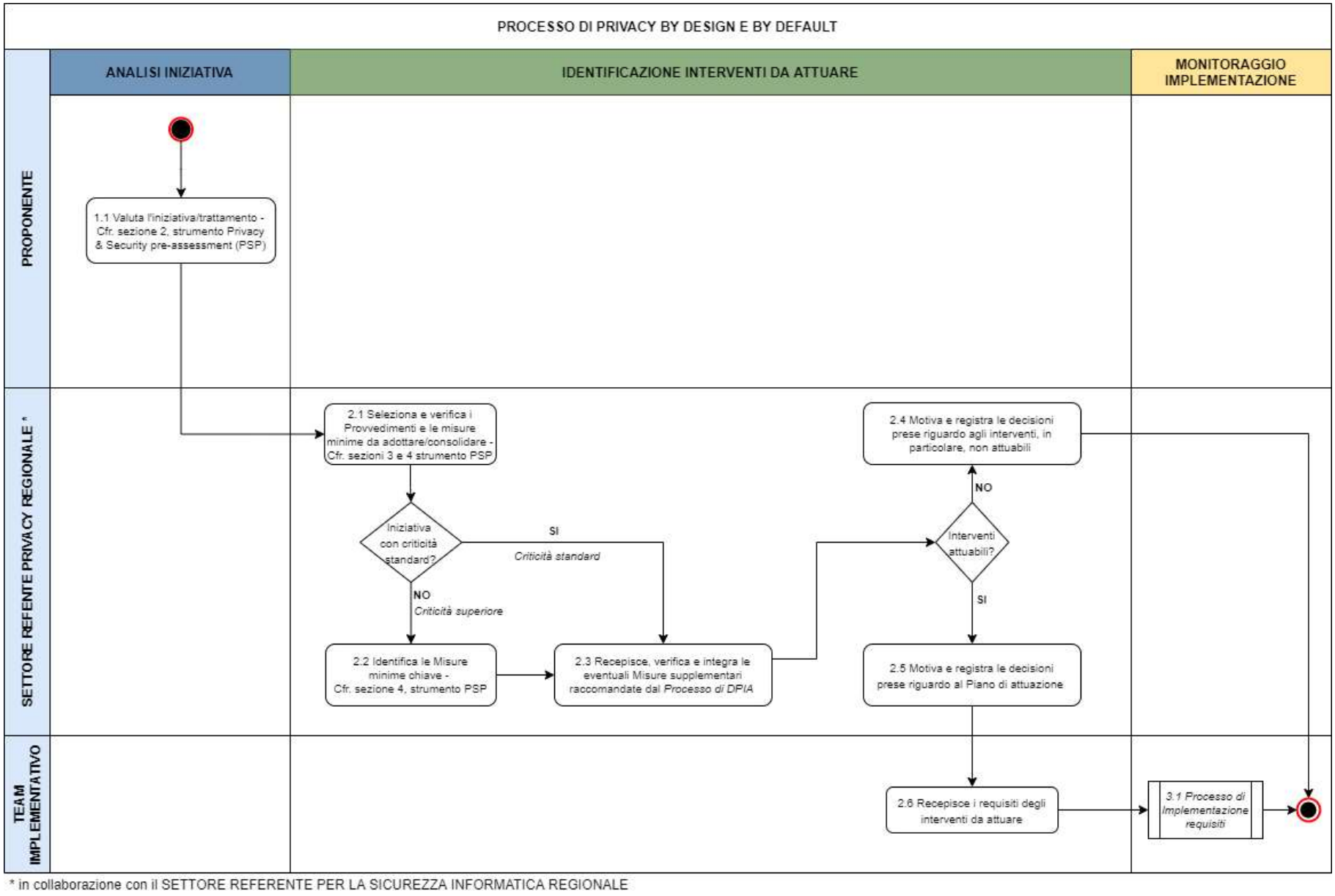


Figura 1 Diagramma del Processo di Privacy by design e by default

Nella tabella sottostante si riporta la legenda dei simboli utilizzati al fine di rappresentare graficamente il Processo di seguito raffigurato e descritto.

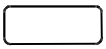
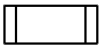
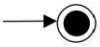
Simbolo	Descrizione
	Blocco attività
	Blocco decisionale
	Blocco di sotto processo
	Inizio flusso
	Fine flusso

Tabella 5 Legenda del diagramma di processo

5.2 Fase 1: Analisi Iniziativa

Descrizione generale

Analisi delle caratteristiche principali dell'iniziativa proposta e valutazione del relativo livello generale di criticità (standard/superiore) riguardo al trattamento dei dati personali

Attori coinvolti

- *Proponente*
- *Settore referente privacy regionale*
- *Settore referente per la sicurezza informatica regionale*

Input della fase

- Nuova[5] iniziativa progettuale, che comporta il trattamento di dati personali di titolarità dell'Ente, o nuovo trattamento nell'ambito di un'iniziativa già avviata

5 Nuova iniziativa o "modifica significativa" di un'iniziativa già avviata

ID	Attività	Descrizione	Output
1.1	Valuta l'iniziativa / trattamento - Cfr. sezione 2, strumento PSP	Il *Proponente* (figura, team o struttura) di una nuova iniziativa, che comporta il trattamento di dati personali di titolarità dell'Ente, o di un nuovo trattamento nell'ambito di un'iniziativa già avviata, procede alla compilazione dello strumento PSP, completando le informazioni di copertina (sezione 1) e rispondendo alle domande del questionario di assessment dell'iniziativa (sezione 2). Tale questionario consente di identificare le principali tipologie di criticità riguardo all'eventuale trattamento di dati personali presente. A conclusione di tale attività sarà possibile determinare: • il livello generale di criticità ("Standard" o "Superiore") dell'iniziativa / trattamento in esame; • la Baseline generale degli interventi necessari per gestire le criticità emerse. <u>*Note*</u> *La Baseline degli interventi riguarda i Provvedimenti del Garante Privacy e le misure minime applicabili secondo AgID*[6]*ed ENISA*[7]*.*	- Questionario di assessment compilato (sezione 2, strumento PSP) - Livello generale di criticità dell'iniziativa / trattamento - Baseline generale degli interventi necessari

Tabella 6 Attività Fase 1: Analisi Iniziativa

5.3 Fase 2: Identificazione Interventi da Attuare

<u>Descrizione generale</u>
Selezione dei provvedimenti e delle misure da adottare o consolidare a tutela dell'iniziativa proposta e verifica della loro fattibilità.

<u>Attori coinvolti</u>
- *Settore referente privacy regionale*
- *Settore referente per la sicurezza informatica regionale*
- *Team implementativo*
- *Proponente*

<u>Input della fase</u>
- Questionario di assessment compilato (sezione 2, strumento PSP)
- Livello generale di criticità dell'iniziativa / trattamento
- Eventuali raccomandazioni dal Processo di DPIA

6 Misure di sicurezza di livello minimo di cui alla circolare AgID n. 2/2017 del 18 aprile 2017
7 Misure tecniche e organizzative di cui all'Allegato A, sezione A.1, del Manuale ENISA sulla Sicurezza nel trattamento dei dati personali (dicembre 2017)

ID	Attività	Descrizione	Output
2.1	Seleziona e verifica i Provvedimenti e le Misure minime da adottare / consolidare - Cfr. sezioni 3 e 4, strumento PSP	Il *Settore referente privacy regionale*, ricevuto il questionario di assessment compilato (sezione 2, strumento PSP), seleziona i provvedimenti e le misure minime effettivamente applicabili all'iniziativa in esame e verifica la loro fattibilità in termini di soluzioni implementative, tempi e costi, con la collaborazione del *Settore referente per la sicurezza informatica regionale*.	- Lista dei requisiti minimi di privacy e sicurezza da attuare
2.2	Identifica le Misure minime chiave - Cfr. sezione 4, strumento PSP	Nel caso l'iniziativa/trattamento riveli un livello di criticità generale "Superiore", il *Settore referente privacy regionale*, con la collaborazione del *Settore referente per la sicurezza informatica regionale*, identifica, nell'ambito della lista dei requisiti minimi, le misure minime chiave in modo da pianificare al meglio le risorse e le priorità degli interventi da mettere in campo.	- Lista dei requisiti minimi di privacy e sicurezza da attuare, con requisiti chiave in evidenza
2.3	Recepisce, verifica e integra le eventuali Misure supplementari raccomandate dal Processo di DPIA	Nel caso il Processo di DPIA raccomandi l'applicazione di specifiche misure tecniche e organizzative per mitigare ulteriormente il rischio, il *Settore referente privacy regionale*, con la collaborazione del *Settore referente per la sicurezza informatica regionale*, recepisce tali misure, selezionando quelle supplementari rispetto alle misure già determinate nell'attività 2.1, e verificandone la fattibilità, in termini di soluzioni implementative, tempi e costi.	- Lista dei requisiti di privacy e sicurezza da attuare (comprensiva di requisiti minimi e requisiti supplementari da DPIA)

ID	Attività	Descrizione	Output
2.4	Motiva e registra le decisioni prese riguardo agli interventi, in particolare, non attuabili	Nel caso in cui gli interventi di sicurezza e privacy previsti (cfr. la Lista dei requisiti complessivi) non siano tutti fattibili, per mancanza di soluzioni che soddisfino i limiti di costo e di tempo ammissibili, il *Settore referente privacy regionale*, con la collaborazione del *Settore referente per la sicurezza informatica regionale*, motiva e registra nello strumento PSP le decisioni prese riguardo agli interventi, in particolare, non attuabili. <u>Note</u> *Ai fini dell'accountability è necessario tracciare le attività svolte e le decisioni intervenute durante il loro svolgimento. Per tale motivo, il file Excel dello strumento PSP relativo all'iniziativa, con tutte le informazioni raccolte sulle attività svolte durante il Processo di Privacy by design e by default, è opportunamente archiviato, insieme ad altra eventuale documentazione a corredo.*	- File dello strumento PSP da archiviare, insieme ad altra eventuale documentaz. a corredo
2.5	Motiva e registra le decisioni prese riguardo al Piano di attuazione	Nel caso in cui gli interventi di sicurezza e privacy previsti (cfr. la Lista dei requisiti complessivi) siano tutti attuabili, il *Settore referente privacy regionale*, con la collaborazione del *Settore referente per la sicurezza informatica regionale*, motiva e registra nello strumento PSP le decisioni prese riguardo agli interventi da mettere in campo. <u>Note</u> *Ai fini dell'accountability è necessario tracciare le attività svolte e le decisioni intervenute durante il loro svolgimento. Per tale motivo, il file Excel dello strumento PSP relativo all'iniziativa, con tutte le informazioni raccolte sulle attività svolte durante il Processo di Privacy by design e by default, è opportunamente archiviato, insieme ad altra eventuale documentazione a corredo.*	- File dello strumento PSP da archiviare, insieme ad altra eventuale documentaz. a corredo

ID	Attività	Descrizione	Output
2.6	Recepisce i requisiti degli interventi da attuare	*Il Team implementativo*, con la collaborazione del *Settore referente privacy regionale* e del *Settore referente per la sicurezza informatica regionale*, recepisce la lista dei requisiti di privacy e sicurezza complessivi, rivedendo le soluzioni implementative inizialmente individuate e condividendo il piano di implementazione. *Note* *Ai fini dell'accountability, il Piano di implementazione è archiviato insieme al file Excel dello strumento PSP relativo all'iniziativa.*	- Piano di implementaz.

Tabella 7 Attività Fase 2: Identificazione Interventi da Attuare

5.4 Fase 3: Monitoraggio Implementazione

Descrizione generale

Monitoraggio dello stato di avanzamento delle attività di implementazione dei requisiti e gestione di eventuali proposte di soluzioni alternative.

Attori coinvolti

- *Team implementativo*
- *Proponente*
- *Settore referente privacy regionale*
- *Settore referente per la sicurezza informatica regionale*

Input della fase

- Lista dei requisiti di privacy e sicurezza da attuare
- Piano di implementazione

ID	Attività	Descrizione	Output
3.1	Conduce il "Processo di Implementazione Requisiti" e ne riporta le informazioni sullo stato di avanzamento	Il *Team implementativo* conduce le attività di implementazione: • consentendo al *Proponente*, al *Settore referente privacy regionale* e al *Settore referente per la sicurezza informatica regionale*, di monitorare lo stato di avanzamento delle attività, informandoli tempestivamente di eventuali scostamenti rispetto al piano di implementazione condiviso; • coinvolgendo il *Settore referente privacy regionale* e il *Settore referente per la sicurezza informatica regionale* nel caso debbano essere considerate proposte di soluzioni alternative (per soddisfare i requisiti) rispetto a quanto inizialmente stabilito. <u>*Note*</u> *Ai fini dell'accountability, le soluzioni implementate, le informazioni sulle eventuali discordanze rispetto a quanto stabilito e la relative lista di test, sono archiviate insieme al file Excel dello strumento PSP relativo all'iniziativa.*	- Lista di test per le soluzioni implementate e dei relativi esiti

Tabella 8 Attività Fase 3: Monitoraggio Implementazione

5.5 Matrice RACI

Di seguito vengono riportati i ruoli e le responsabilità[8] degli attori coinvolti per ciascuna attività del Processo sopra descritto.

	Valuta l'iniziativa/trattamento	Seleziona e verifica i Provvedimenti e le Misure minime da adottare/consolidare	Identifica le Misure minime chiave	Recepisce, verifica e integra le eventuali Misure supplementari raccomandate dal Processo di DPIA	Verifica i Provvedimenti e le Misure minime da attuare (incluse quelle chiave)	Motiva e registra le decisioni prese riguardo agli interventi, in particolare, non attuabili	Motiva e registra le decisioni prese riguardo al Piano di attuazione	Recepisce i requisiti degli interventi da attuare	Conduce il "Processo di Implementazione Requisiti" e ne riporta le informazioni sullo stato di avanzamento
Proponente	A/R	I	I	I	I	I	I	I	I
Settore referente privacy regionale	C	A/R	A/R	A/R	A/R	A/R	A/R	C	C
Settore referente per la sicurezza informatica regionale	C	R	R	R	R	R	R	C	C
Team implementativo								A/R	A/R

Figura 2 Matrice RACI del Processo di Privacy by design e by default

8 Responsable (R) = Indica il responsabile della realizzazione, cioè colui che esegue materialmente un'attività mediante una responsabilità di tipo operativo
Accountable (A) = Indica colui che viene riconosciuto come l'accentratore della responsabilità finale di una certa attività. È la persona che ha l'ultima parola e il potere di veto
Consulted (C) = Indica la persona consultata prima di eseguire l'attività o prima di prendere decisioni esecutive
Informed (I) = Chi viene informato, di solito successivamente, della decisione o dell'azione intrapresa e/o viene chiamato a collaborare alla realizzazione della soluzione

6 ALLEGATO 1 - STRUMENTO A SUPPORTO DEL PROCESSO

Il presente lavoro è stato corredato di uno strumento a supporto di tutte le fasi di attività previste per il Processo di Privacy by design e by default. Tale strumento, basato su MS Excel e denominato "Privacy & Security Pre-Assessment (PSP)", è riportato separatamente nell'Allegato 1 del presente deliverable.

6.1 Lo strumento Privacy & Security Pre-Assessment (PSP)

Lo strumento "Privacy & Security Pre-Assessment (PSP)" si compone di differenti sezioni (ognuna corrispondente ad uno specifico sheet del relativo file Excel):

- Copertina (sezione "1.Cover")
- Questionario di assessment (sezione "2.Assessment");
- Provvedimenti (sezione "3.Provvedimenti");
- Misure minime (sezione "4.MisureMinime");
- Dashboard provvedimenti (sezione "Dashboard-Provv");
- Dashboard misure minime (sezione "Dashboard-Misure").

6.2 Criteri e modalità di utilizzo

6.2.1 Sezione "1.Cover"

All'interno di questa sezione dovranno essere specificati:

- il nome e la tipologia della nuova Iniziativa/Trattamento;
- i riferimenti della persona, del team o della struttura che richiedono di valutare i requisiti di privacy e sicurezza della nuova Iniziativa/Trattamento;
- il referente della compilazione del file;
- lo stato della compilazione e la data dell'ultimo aggiornamento;
- i validatori dei contenuti inseriti.

Il campo "Stato Compilazione" riporta in automatico la voce "Compilato" solo se si compila almeno il campo "Tipologia Iniziativa\Trattamento" della sezione "1.Cover" e tutte e 16 le domande riportate nella sezione "2.Assessment". In tutti gli altri casi il campo "Stato Compilazione" riporterà la voce "In fase di compilazione".

Al termine della compilazione del file, dovranno essere riportati nella sezione "1.Cover" anche i riferimenti di uno o più validatori dei contenuti inseriti.

LEONARDO / NTT DATA

Privacy & Security Pre-Assessment (PSP)

Nome Iniziativa\Trattamento	
Tipologia Iniziativa\Trattamento	
Proponente	
Referente Compilazione	
Stato Compilazione	<Campo compilato automaticamente (inserire il nome dell'iniziativa o del trattamento)>
Data Ultimo Aggiornamento	
Validatori Compilazione	

Allegato 1 "Strumento a supporto del processo" del deliverable D01_SCO.1_FASE1 "Processo di Privacy by design e by default"

Versione 2.0

Figura 3 Strumento PSP / Sezione 1

6.2.2 Sezione "2.Assessment"

All'interno di questa sezione dovranno essere fornite tutte le informazioni necessarie per la valutazione della criticità generale dell'iniziativa, riguardo al trattamento dei dati personali, rispondendo a 16 specifiche domande.

1. L'iniziativa in esame prevede il trattamento di dati personali?
2. Quali categorie di dati personali sono coinvolte?
3. Chi sono i soggetti interessati al trattamento?
4. Come sono raccolti i dati personali?
5. Quali sono le finalità del trattamento?
6. Chi è il Delegato del Titolare del trattamento?
7. Sono coinvolte terze parti (es. fornitori, consulenti, etc.)?
8. Quali sono gli ambiti di coinvolgimento delle terze parti?
9. Qual è il volume di dati personali raccolti?
10. Quali sono i supporti attraverso cui vengono raccolti i dati personali?
11. Quali sono le modalità di archiviazione dei dati?
12. In quale Paese avviene il trattamento?
13. Chi potrà accedere ai dati personali?
14. Quanti sono gli utenti che utilizzeranno i servizi erogati?
15. Quali sono le modalità di accesso ai servizi erogati?
16. L'iniziativa prevede l'utilizzo di tecnologie innovative? (Specificare quali)

Le risposte a tali domande saranno fornite e giustificate (ai fini dell'accountability) dal Proponente.

A seguito della compilazione del questionario di assessment, lo strumento determinerà il livello generale di criticità dell'iniziativa visualizzando uno dei seguenti messaggi:

- Livello di criticità STANDARD;
- Livello di criticità SUPERIORE;
- Livello di criticità NON DEFINITO.

Il calcolo del livello generale di criticità segue delle logiche predefinite che tengono conto della criticità specifica di ogni singola caratteristica dell'iniziativa investigata attraverso le domande del questionario.

In corrispondenza del livello generale di criticità, lo strumento visualizzerà anche una serie di indicazioni utili per procedere con le attività.

Nr.	Domande	Risposte	Note
1	**L'iniziativa in esame prevede il trattatamento di dati personali?**		
2	**Quali categorie di dati personali sono coinvolte?**	☐ Dati di identificazione personale (anche da videosorveglianza) / di contatto / documenti di identificazione ☐ Dati sull'istruzione e competenze / occupazione lavorativa / situazione familiare ☐ Dati economici / finanziari / fiscali ☐ Dati di navigazione in rete ☐ Dati di localizzazione GPS ☐ Dati sullo stato di salute / vita / orientamento sessuale ☐ Dati sull'origini razziali o etniche / opinioni politiche / convinzioni religiose o filosofiche / appartenenza sindacale ☐ Dati genetici ☐ Dati biometrici ☐ Dati su condanne penali e reati ☐ Dati relativi a firme digitali ☐ Altro (specificare nel campo Note)	
3	**Chi sono i soggetti interessati al trattamento?**	☐ Dipendenti di Regione Calabria ☐ Personale di enti pubblici ☐ Revisori / membri di organismi di controllo ☐ Personale di strutture sanitarie ☐ Personale di enti / società privati ☐ Collaboratori / professionisti esterni ☐ Cittadini ☐ Candidati a posizioni lavorative ☐ Iscritti ad albi o elenchi ☐ Pazienti ☐ Soggetti vulnerabili (minori, anziani, disabili etc.) ☐ Altro (specificare nel campo Note)	
4	**Come sono raccolti i dati personali?**	☐ Dati forniti dall'interessato ☐ Dati forniti da soggetto privato diverso dall'interessato ☐ Dati forniti da soggetto pubblico ☐ Indirettamente attraverso banche dati pubbliche ☐ Tramite strumenti di lavoro ☐ Tramite migrazione dei dati da altro sistema aziendale ☐ Altro (specificare nel campo Note)	
5	**Quali sono le finalità del trattamento?**	☐ Abilitazione e gestione piattaforme regionali e ministeriali ☐ Accreditamenti / Autorizzazioni ☐ Adempimenti ad obblighi di legge ☐ Adempimenti amministrativi connessi all'attività di monitoraggio, controllo e vigilanza di enti pubblici, società, fondazioni, etc. ☐ Adempimenti connessi al procedimento amministrativo ☐ Adempimenti connessi alla gestione dei finanziamenti agevolati ☐ Adempimenti connessi alla gestione del collocamento mirato ☐ Adempimenti connessi alla gestione di ammortizzatori sociali / precariato / politiche attive ☐ Adempimenti in materia di privacy ☐ Adempimenti in materia di trasparenza ☐ Attività di comunicazione POR ☐ Attività di controllo ☐ Attività di verifica - monitoraggio - controllo fondi POR ☐ Contratti ☐ Controllo accessi ☐ Emergenza Covid-19 ☐ Gestione assicurativa ☐ Gestione contabilità ☐ Gestione contributi ☐ Gestione corrispondenza ☐ Gestione CPI ☐ Gestione d.lgs. 81/2008 - salute e sicurezza sul lavoro ☐ Gestione decreti e delibere ☐ Gestione del contenzioso ☐ Gestione del personale ☐ Gestione gare d'appalto / fornitori ☐ Gestione patrimoniale ☐ Gestione piani territoriali ☐ Gestione previdenziale - retribuzioni ☐ Gestione progetti ☐ Gestione rimborso spese / spese mediche ☐ Gestione soggetti vulnerabili ☐ Gestione strutture socio-sanitarie ☐ Gestione tasse ☐ Gestione urgenze (Prot. Civ.) ☐ Gestione volontariato e terzo settore ☐ Partecipazione ad avvisi pubblici ☐ Prestiti ☐ Profilazione (anche on line) ☐ Ricerca statistica ☐ Sanzioni ☐ Selezione del personale ☐ Tutela dipendenti - legge 179/2017 ☐ Altro (specificare nel campo Note)	
6	**Chi è il Delegato del Titolare del trattamento?**	<inserire i riferimenti del Delegato>	
7	**Sono coinvolte terze parti (es. fornitori, consulenti, etc.)?**		
8	**Quali sono gli ambiti di coinvolgimento delle terze parti?**	☐ Manutenzioni di applicazioni informatiche ☐ Manutenzioni di infrastrutture ☐ Servizi di help desk ☐ Servizi erogati sul territorio ☐ Servizi socio-sanitari ☐ Attività no profit ☐ Attività connesse a concessioni ☐ Consulenze legali ☐ Attività di audit ☐ Revisioni di bilancio ☐ Altro (specificare nel campo Note)	
9	**Qual è il volume di dati personali raccolti?**	☐ Fino a 100 ☐ Fino a 1.000 ☐ Fino a 10.000 ☐ Oltre 10.000	
10	**Quali sono i supporti attraverso cui vengono raccolti i dati personali?**	☐ Supporti elettronici ☐ Supporti cartacei ☐ Altro (specificare nel campo Note)	
11	**Quali sono le modalità di archiviazione dei dati?**	☐ Archivi fisici a lungo termine presso l'ente ☐ Archivi fisici a lungo termine presso terze parti ☐ Archivi fisici a breve termine presso l'ente (es. ufficio persone autorizzate, etc.) ☐ Archivi fisici a breve termine presso terze parti ☐ Archivi informatici presso l'ente (es. sistema informatico specifico, cartella di rete condivisa, postazione di lavoro personale, etc.) ☐ Archivi informatici presso terze parti ☐ Cloud privato dell'ente ☐ Cloud privato di terze parti ☐ Cloud pubblico contrattualizzato dall'ente ☐ Cloud pubblico contrattualizzato da terze parti ☐ Altro (specificsre nel campo Note)	
12	**In quale Paese avviene il trattamento?**	☐ Esclusivamente in Italia ☐ Esclusivamente in UE ☐ Esclusivamente extra UE / Parzialmente extra UE	
13	**Chi potrà accedere ai dati personali?**	☐ Strutture interne all'ente ☐ Privati che lavorano presso l'ente ☐ Privati che lavorano presso la propria sede ☐ Autorità giudiziarie e forze dell'ordine ☐ Enti pubblici ☐ Organi di vigilanza e controllo ☐ Altro (specificare nel campo Note)	
14	**Quanti sono gli utenti che utilizzeranno i servizi erogati?**	☐ Fino a 100 ☐ Fino a 1.000 ☐ Fino a 10.000 ☐ Oltre 10.000	
15	**Quali sono le modalità di accesso ai servizi erogati?**	☐ Fruizione cartacea ☐ Internet ☐ Rete interna ☐ Applicazione mobile ☐ Telefono ☐ E-mail ☐ Messaggistica istantanea ☐ Altro (specificare nel campo Note)	
16	**L'iniziativa prevede l'utilizzo di tecnologie innovative? (Specificare quali)**	☐ Dispositivi contactless (es. RFID, NFC, etc.) ☐ Dispositivi di riconoscimento biometrico (es. impronta digitale, iride, etc.) ☐ Sensori IoT (Internet of Things) ☐ Sistemi di videosorveglianza intelligenti ☐ Token ☐ Smart card ☐ Altro (specificare nel campo Note)	

Livello di criticità NON DEFINITO

Indicazioni

1) Non si prevedono trattamenti di dati personali.

Baseline interventi

Provvedimenti

Misure minime di sicurezza

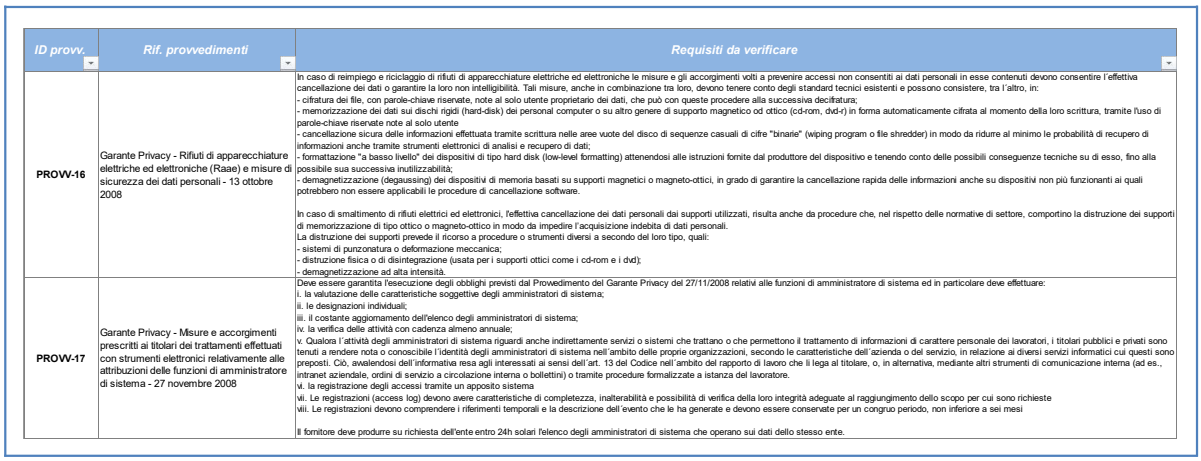
Figura 4 Strumento PSP / Sezione 2

6.2.3 Sezione “3.Provvedimenti”

All’interno di questa sezione, elaborata facendo clic sul pulsante “Provvedimenti” della sezione “2.Assessment”, sarà possibile visualizzare e gestire i Provvedimenti emanati dal Garante Privacy italiano e/o derivati da pareri di “Working Party” (cfr. WP105, WP249, etc.). Tali Provvedimenti sono opportunamente selezionati in funzione delle risposte fornite nel questionario di assessment.

Per ogni Provvedimento ammissibile sarà possibile, inoltre, annotare le principali informazioni riguardo al relativo stato di attuazione, ovvero:

- Intervento previsto (da adottare, da consolidare, già adottato, non applicabile);
- Responsabile interno\esterno del piano di rientro;
- Data di inizio e Data di fine del piano di rientro;
- Annotazioni varie.



ID provv.	Rif. provvedimenti	Requisiti da verificare
PROVV-16	Garante Privacy - Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008	In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti devono consentire l’effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l’altro, in: - cifratura dei file, con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura; - memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l’uso di parole-chiave riservate note al solo utente - cancellazione sicura delle informazioni effettuata tramite scrittura nelle aree vuote del disco di sequenze casuali di cifre “binarie” (wiping program o file shredder) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati; - formattazione “a basso livello” dei dispositivi di tipo hard disk (low-level formatting) attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità; - demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software. In caso di smaltimento di rifiuti elettrici ed elettronici, l’effettiva cancellazione dei dati personali dai supporti utilizzati, risulta anche da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l’acquisizione indebita di dati personali. La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali: - sistemi di punzonatura o deformazione meccanica; - distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd); - demagnetizzazione ad alta intensità.
PROVV-17	Garante Privacy - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008	Deve essere garantita l’esecuzione degli obblighi previsti dal Provvedimento del Garante Privacy del 27/11/2008 relativi alle funzioni di amministratore di sistema ed in particolare deve effettuare: i. la valutazione delle caratteristiche soggettive degli amministratori di sistema; ii. le designazioni individuali; iii. il costante aggiornamento dell’elenco degli amministratori di sistema; iv. la verifica delle attività con cadenza almeno annuale; v. Qualora l’attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l’identità degli amministratori di sistema nell’ambito delle proprie organizzazioni, secondo le caratteristiche dell’azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell’informativa resa agli interessati ai sensi dell’art. 13 del Codice nell’ambito del rapporto di lavoro che li lega al titolare, o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini) o tramite procedure formalizzate a istanza del lavoratore. vi. la registrazione degli accessi tramite un apposito sistema vii. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste viii. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell’evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi Il fornitore deve produrre su richiesta dell’ente entro 24h solari l’elenco degli amministratori di sistema che operano sui dati dello stesso ente.

Figura 5 Strumento PSP / Sezione 3

6.2.4 Sezione “4.MisureMinime”

All’interno di questa sezione, elaborata facendo clic sul pulsante “Misure minime di sicurezza” della sezione “2.Assessment”, sarà possibile visualizzare e gestire le misure minime di sicurezza stabilite da AgID[9] ed ENISA[10]. Le misure di sicurezza chiave sono opportunamente evidenziate in funzione delle risposte fornite nel questionario di assessment.

Per ogni misura di sicurezza indicata sarà possibile, inoltre, annotare le principali informazioni riguardo al relativo stato di attuazione, ovvero:

- Intervento previsto (da adottare, da consolidare, già adottato, non applicabile);
- Responsabile interno\esterno del piano di rientro;
- Data di inizio e Data di fine del piano di rientro;
- Annotazioni varie.

9 Misure di sicurezza di livello minimo di cui alla circolare AgID n. 2/2017 del 18 aprile 2017
10 Misure tecniche e organizzative di cui all’Allegato A, sezione A.1, del Manuale ENISA sulla Sicurezza nel trattamento dei dati personali (dicembre 2017)

ID misure	Descrizione misure da verificare	Motivazioni baseline
ABSC-01.01.01	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)
ABSC-01.03.01	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)
ABSC-01.04.01	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)
ABSC-02.01.01	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)
ABSC-02.03.01	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)
ABSC-03.01.01	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi	Misura obbligatoria AgID (cfr. circolare AgID n. 2/2017 del 18 aprile 2017)

Figura 6 Strumento PSP / Sezione 4

6.2.5 Sezione "Dashboard-Provv"

All'interno di questa sezione saranno disponibili informazioni di sintesi sullo stato di implementazione dei Provvedimenti (da adottare, da consolidare, già adottati, non applicabili).

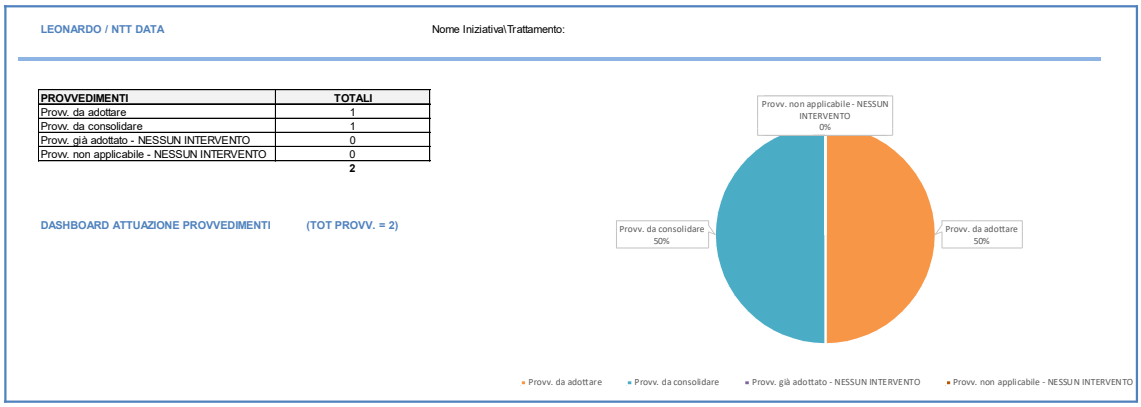


Figura 7 Strumento PSP / Sezione dashboard provvedimenti

6.2.6 Sezione "Dashboard-Misure"

All'interno di questa sezione saranno disponibili informazioni di sintesi sullo stato di implementazione dei delle misure minime di sicurezza (da adottare, da consolidare, già adottate, non applicabili).

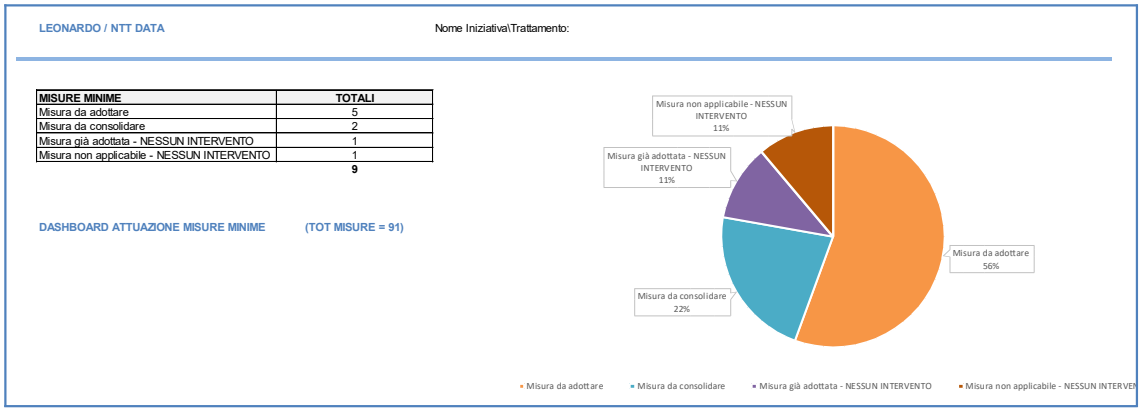


Figura 8 Strumento PSP / Sezione dashboard misure minime

6.3 Verifiche a cura del RPD

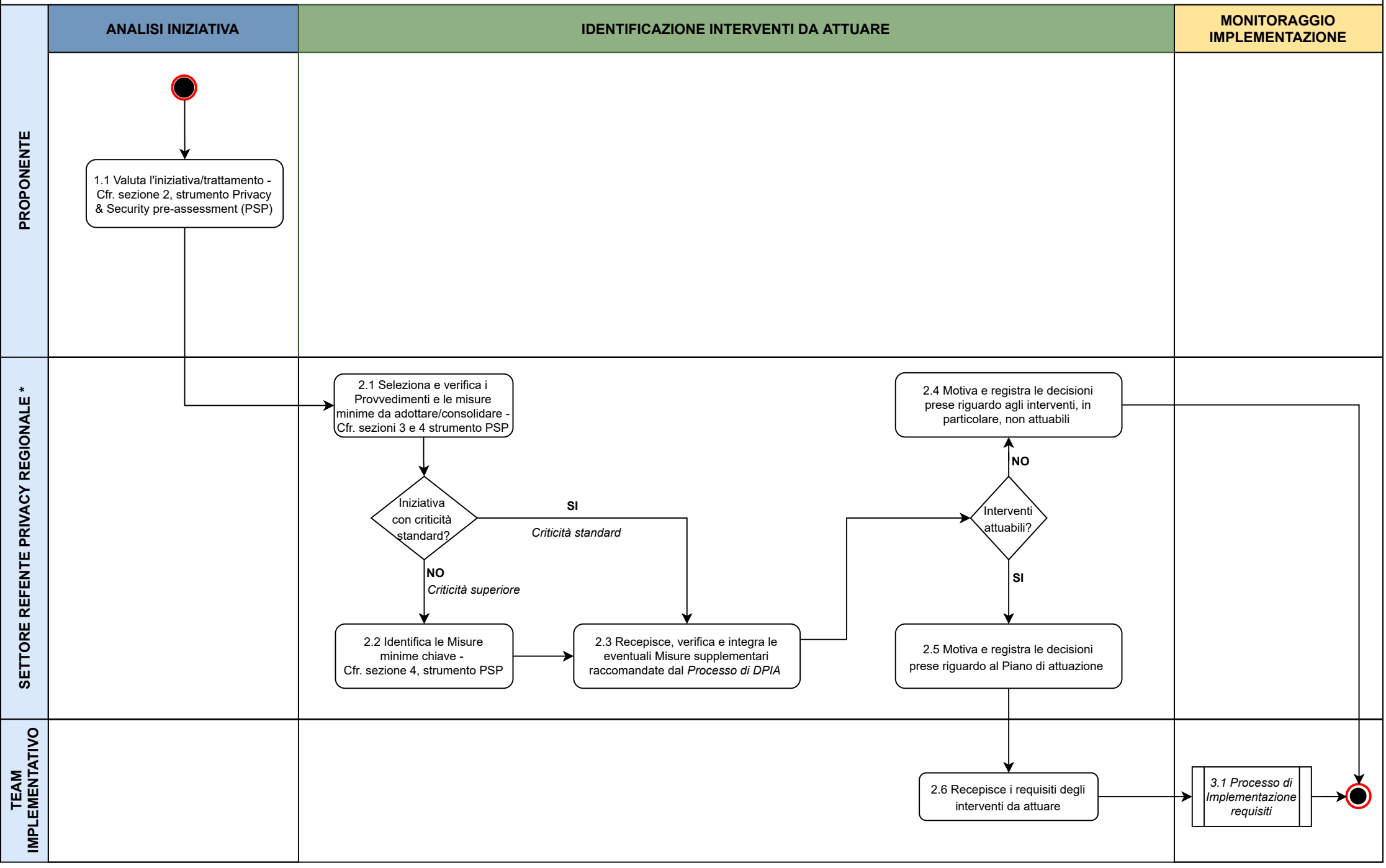
Il Responsabile della Protezione dei Dati potrà effettuare verifiche a campione, a sostegno dell'accountability del Titolare, su tutte le attività previste dal presente Processo, richiedendo l'accesso alle informazioni registrate nello strumento "Privacy & Security Pre-Assessment (PSP)". Alcune di tali verifiche potranno riguardare in particolare:

- la corretta compilazione del questionario di assessmemt da parte del Proponente;
- la corretta selezione dei provvedimenti e delle misure minime di sicurezza applicabili;
- l'adeguatezza delle giustificazioni riportate riguardo alla non applicabilità di alcuni requisiti;
- la coerenza degli interventi eseguiti/in corso rispetto al piano dei lavori.

7 ALLEGATO 2 - DOCUMENTO DI RAPPRESENTAZIONE DEL PROCESSO

Al fine di consentire una migliore lettura e consultazione del diagramma del *Processo* descritto nel presente documento, si allega una versione dello stesso in formato pdf.

PROCESSO DI PRIVACY BY DESIGN E BY DEFAULT



* in collaborazione con il SETTORE REFERENTE PER LA SICUREZZA INFORMATICA REGIONALE