Identificativo: <<RC_PG_PD_01_Documento di attuazione dei principi di Privacy by Design & by Default >>

<<Ver. 1.0>>

Data: 30/10/2024

PROGETTO:

GOVERNO DELLA CYBERSECURITY

E DELLA DATA PROTECTION

Documento di attuazione dei principi Privacy by Design & Privacy by Default

Lista di Distribuzione

Rev.	Data	Destinatario	Ente/Azienda
1.0	30/10/2024	Ing. Alfredo Pellicanò	Regione Calabria
1.0	30/10/2024	Dott.ssa Paola Zuccaro	Regione Calabria
1.0	30/10/2024	Ing. Giovanna Pisano	Regione Calabria
1.0	30/10/2024	Ing. Sebastiano Massimo Rodà	Regione Calabria
1.0	30/10/2024	Avv. Angela Stellato	Regione Calabria
1.0	30/10/2024	Dott. Salvatore Lopresti	Regione Calabria
1.0	30/10/2024	Avv. Daniela Labate	Regione Calabria
1.0	30/10/2024	Avv. Giovanni Sacchi	Regione Calabria
1.0	30/10/2024	Dott.ssa Ilenia Pia Viceconti	Deloitte
1.0	30/10/2024	Dott.ssa Alessia Ruta	Deloitte

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autore di rif.
1.0	30/10/2024	Prima emissione	Dip. Transizione Digitale ed Attività Strategiche

Calendario degli Incontri Principali

Data	Incontro	Stato
16/09/2024	Riunione con il DPO Avv. Angela Stellato e Avv. Giovanni Sacchi	Effettuato
07/10/2024	Riunione con il DEC del Progetto Ing. Giovanna Pisano	Effettuato
23/10/2024	Riunione con il DEC del Progetto Ing. Giovanna Pisano	Effettuato
28/10/2024	Riunione con il DEC del Progetto Ing. Giovanna Pisano	Effettuato

SOMMARIO

1. INTRODUZIONE

Il Regolamento UE n. 679/2016 “Regolamento Generale sulla Protezione dei Dati” (di seguito “GDPR” o “Regolamento”) impone al Titolare del trattamento l'adozione di misure tecniche e organizzative adeguate volte a tutelare i Dati Personali da trattamenti illeciti.

L'articolo 25 del Regolamento, in particolare, introduce il principio di Privacy by Design e Privacy by Default, un approccio concettuale innovativo che impone al Titolare del trattamento l'obbligo di avviare un progetto prevedendo, fin da subito, l’adozione di misure volte a tutelare i Dati Personali per impostazione predefinita.

In particolare, il GDPR stabilisce che la Privacy by Design (protezione dei dati fin dalla progettazione) permette una protezione dei dati fin dal disegno o progettazione di un trattamento che ha ad oggetto dati personali.

Con la Privacy by Default (protezione dei dati per impostazione predefinita) il GDPR stabilisce che il Titolare deve trattare solo i dati che ritiene necessari e sufficienti per perseguire le finalità previste, nel lasso temporale strettamente necessario a tali fini.

Pertanto, la protezione dei Dati Personali non deve più essere considerata come un adempimento di mera compliance che interviene ex post sulle eventuali lacune o deficit presenti nel sistema di gestione dei Dati Personali, ma deve essere considerata parte integrante dei processi interni, fin dalla nascita degli stessi e sino alla conclusione del ciclo di vita del dato.

I principi di Privacy by Design e by Default cui devono attenersi i Dipartimenti e le Strutture Equiparate di Regione Calabria, abilitano, quindi, un approccio “Privacy Embedded” ossia di “Privacy incorporata”. Tale approccio è volto all’integrazione ex-ante delle logiche di Data Protection, che obbliga il Titolare, nella fase iniziale di determinazione delle finalità e delle modalità del trattamento, a valutare i rischi alla luce dell’ambito specifico di applicazione delle tecnologie disponibili, mettendo in atto le misure tecnico-organizzative che garantiscano un’adeguata tutela agli interessati.

1.1 SCOPO

Lo scopo del presente documento è illustrare i principi generali ed operativi di Privacy by Design e by Default, per garantire la tutela degli interessati fin dalle fasi di progettazione di ogni nuovo progetto/ trattamento/ processo che prevede un trattamento di Dati Personali da parte dei Dipartimenti e delle Strutture Equiparate di Regione Calabria.

L’adozione dei principi di Privacy by Design e by Default, infatti, offre i seguenti vantaggi:

- l’identificazione immediata delle potenziali criticità in ottica Privacy già nella fase iniziale di disegno di un nuovo progetto, prodotto, servizio, con conseguente riduzione dei costi;
- la maggiore conformità a prescrizioni normative durante lo sviluppo dei progetti e tutela dei diritti e delle libertà degli interessati;
- l’aumento della consapevolezza e sensibilità in materia di protezione dei Dati Personali all’interno dei Dipartimenti e delle Strutture Equiparate di Regione Calabria;
- il consolidamento del rapporto di fiducia tra l’interessato e il Titolare del trattamento.

1.2 CAMPO DI APPLICAZIONE

L'ambito di applicazione del presente documento è limitato a quanto oggetto del Regolamento UE n. 679/2016 "Regolamento Generale sulla Protezione dei Dati" ed in particolar modo a quanto espresso all'interno dei seguenti articoli:

- Articolo 25 del GDPR: *"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita";*
- Articolo 32 del GDPR: *"Sicurezza del trattamento"*;
- Articolo 35 del GDPR: *"Valutazione d'impatto sulla protezione dei dati"*.

Inoltre, si tiene conto altresì di ciò che è espresso nel "Processo di Privacy by Design e by Default per la Regione Calabria", approvato con Decreto Dirigenziale n. 10388 del 14 ottobre 2021[7]. Tale Decreto indica le modalità operative nel processo di gestione della Privacy by Design e by Default in coerenza alla ripartizione dei ruoli e competenze, con riferimento alle modalità di gestione dei diritti degli interessati previste nel Regolamento Regionale n. 20 del 18 dicembre 2018, modificato dalla Deliberazione di Giunta Regionale n. 29 del 1° febbraio 2021[5], nonché con le indicazioni fornite dal Garante per la Protezione dei Dati Personali.

2. DEFINIZIONE E ACRONIMI

2.1 DEFINIZIONI

Termine	Descrizione
Privacy by Design	Richiede che la tutela dei diritti e delle libertà degli interessati rispetto al trattamento dei Dati Personali comporti l'attuazione di adeguate misure tecniche e organizzative sia nella fase di progettazione che di esecuzione del trattamento stesso, in ossequio alle disposizioni del Regolamento UE n. 679/2016.
Privacy by Default	Richiede che una volta che un prodotto o un servizio è stato rilasciato al pubblico, le impostazioni di Privacy più rigorose dovrebbero essere applicate per impostazione predefinita, senza alcun input manuale da parte dell'utente finale. Il Titolare del trattamento garantisce che, per impostazione predefinita, siano trattati solo i dati personali necessari a perseguire le finalità indicate. Inoltre, i Dati Personali forniti dall'utente, per consentire l'uso ottimale di un prodotto, devono essere conservati solo per il tempo strettamente necessario a fornire il prodotto o servizio. Se vengono divulgate più informazioni del necessario per fornire il servizio, la "Privacy per impostazione predefinita" è stata violata.
Titolare del trattamento di Dati Personali	Il Titolare del trattamento è 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. Nel caso di specie il Titolare è Regione Calabria.
Misure di sicurezza	Misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei dati personali trattati adeguato al rischio.
Art. 25	1. *"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."* 2. *"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*

Termine	Descrizione
	Personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.[…]"
Art. 32	1. *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:* *a) la pseudonimizzazione e la cifratura dei Dati Personali;* *b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;* *c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;* *d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.* *Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati. […]"*
Art. 35	1. *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."* 2. *"Il Titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.[…]"*

2.2 ACRONIMI

Termine	Descrizione
Regolamento/ GDPR	Regolamento UE n. 679/2016 - General Data Protection Regulation
DPIA	Data Protection Impact Assessment (Valutazione di impatto sulla protezione dei dati)
RPD/DPO	Responsabile per la Protezione dei Dati Personali/ Data Protection Officer

3. RIFERIMENTI

3.1 DOCUMENTI APPLICABILI

Rif.	Codice	Titolo
DA-1.	PG_2024_00P	Piano di Lavoro
DA-2.	CIG 8884642E81	Contratto Esecutivo del 05/03/2024

3.2 DOCUMENTI DI RIFERIMENTO

Rif.	Codice	Titolo
DR-1.	GDPR n. 679/2016	Regolamento UE n. 679/2016 “Regolamento Generale sulla Protezione dei Dati”
DR-2.	ISO/IEC 29100:2011 /Amd 1:2018	Standard ISO/IEC 29100:2011 /Amd 1:2018 – Privacy Framework
DR-3.	DGR N. 29 del 1 febbraio 2021	Regolamento Regionale n. 20 del 18 dicembre 2018 modificato dalla deliberazione di Giunta Regionale n. 29 del 1 febbraio 2021
DR-4.	DD n. 6786 del 30 giugno 2021	Regione Calabria, Decreto Dirigenziale n. 6786 del 30 giugno 2021, “Approvazione della metodologia di valutazione d’impatto per la protezione dei dati personali (DPIA) per la Regione Calabria del 23 marzo 2021”
DR-5.	DD n. 10388 del 14 ottobre 2021	Regione Calabria, Decreto Dirigenziale n. 10388 del 14 ottobre 2021, “Approvazione del processo di gestione della Privacy by Design e by Default della Regione Calabria”
DR-6.	D05-1_SCO.2_FASE1 del 1 settembre 2021	Regione Calabria, “Analisi della compliance rispetto alle misure di sicurezza obbligatorie AgID”
DR-7.	REGCAL-MM del 1 settembre 2021	Modulo di implementazione delle misure minime di sicurezza ICT di Regione Calabria
DR-8.	D05-1_SCO.2_FASE3 del 31 marzo 2022	Politica generale per la sicurezza informatica di Regione Calabria
DR-9.	DGR N. 12 del 14 dicembre 2022	Regolamento Regionale n. 12/2022 e ss.mm.ii "Regolamento di organizzazione delle strutture della Giunta Regionale" (ultima modifica 28/12/2023)
DR-10	DGR N. 2349 del 09 marzo 2021	Decreto Dirigenziale di Regione Calabria n°. 2349 del 09 marzo 2021“Approvazione processo di

Rif.	Codice	Titolo
		gestione Data Breach (incidenti di sicurezza dati Regione Calabria)".

4. RIFERIMENTI NORMATIVI

Il presente documento è redatto in coerenza con le seguenti normative e documenti di riferimento:

[1] Regolamento UE n. 679/2016 - General Data Protection Regulation (di seguito GDPR);
[2] D. Lgs. 196/2003 - Codice in materia di protezione di Dati Personali (di seguito "Codice Privacy");
[3] D. Lgs. 101/2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati);
[4] Standard ISO/IEC 29100:2011 /Amd 1:2018 - "Information technology - Security techniques - Privacy framework";
[5] Regolamento Regionale n. 20 del 18 dicembre 2018 sulle "Competenze in materia di trattamento di Dati Personali" modificato dalla Deliberazione di Giunta Regionale n. 29 del 1 febbraio 2021;
[6] Decreto Dirigenziale di Regione Calabria n. 6786 del 30 giugno 2021 che ha approvato il documento "Metodologia di valutazione d'impatto per la protezione dei dati personali (DPIA)";
[7] Decreto Dirigenziale di Regione Calabria n. 10388 del 14 ottobre 2021 "Approvazione del processo di gestione della Privacy by Design e by Default per la Regione Calabria";
[8] "Analisi della compliance rispetto alle misure di sicurezza obbligatorie AgID" della Regione Calabria del 1° settembre 2021;
[9] "Modulo di implementazione delle misure minime di sicurezza ICT di Regione Calabria" del 1° settembre 2021 in ovvietà alla Circolare AgID n.2/2017 del 18 aprile 2017 "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni;
[10] "Politica generale per la sicurezza informatica di Regione Calabria" del 31 marzo 2022;
[11] DGR N. 12 del 14 dicembre 2022 Regolamento Regionale n. 12/2022 e ss.mm.ii "Regolamento di organizzazione delle strutture della Giunta Regionale" (ultima modifica 28 dicembre 2023);
[12] Decreto Dirigenziale di Regione Calabria n°. 2349 del 09 marzo 2021 "Approvazione processo di gestione Data Breach (incidenti di sicurezza dati Regione Calabria)".

5. PRINCIPI

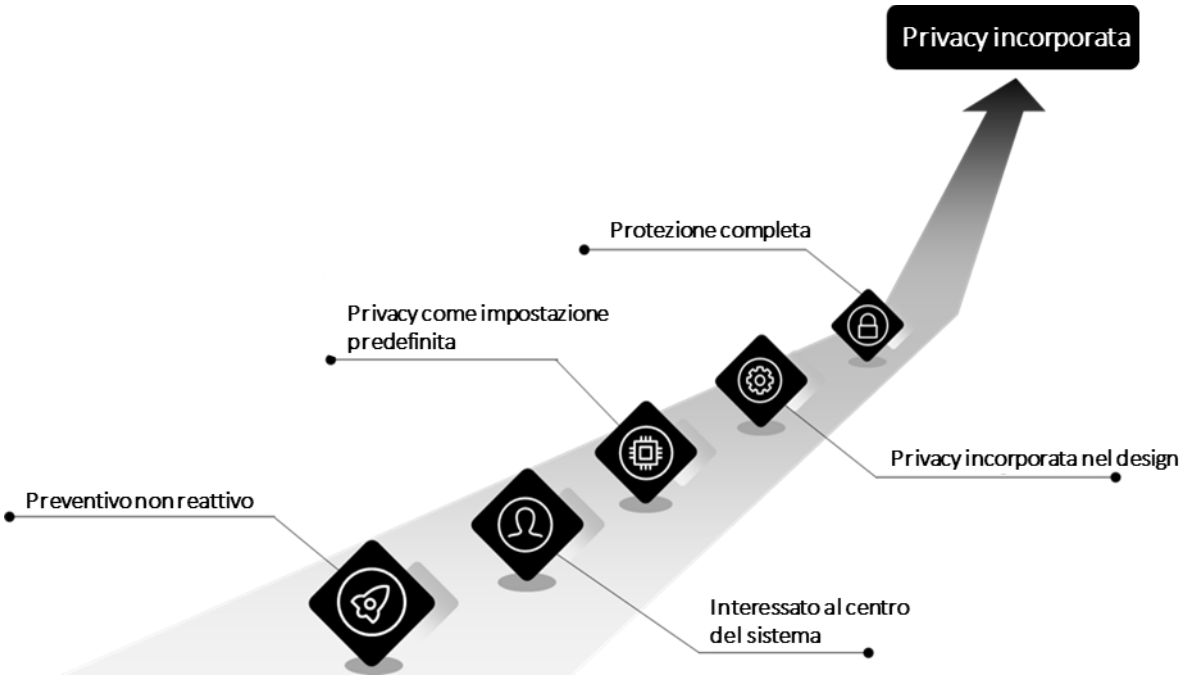
5.1 PRINCIPI GENERALI

L'approccio Privacy by Design e by Default si fonda su una serie di **principi generali** che posizionano l'interessato al centro di ogni nuovo progetto/ trattamento/ processo sin dalle prime fasi di progettazione, così da anticipare e prevenire l'insorgenza successiva di potenziali violazioni dei suoi diritti e delle sue libertà.

I riferimenti normativi di Privacy by Design e by Default trovano riscontro nell'art. 25 del GDPR che, in sintesi, prevede che:

- siano poste in essere misure tecniche e organizzative adeguate volte a attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento stesso e tutelare i diritti degli interessati;
- siano messe 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, garantendo che, per impostazione predefinita, non siano resi accessibili Dati Personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Di seguito, si delineano i principi che i Dipartimenti e le Strutture Equiparate di Regione Calabria devono seguire al fine di sviluppare un approccio di "Privacy incorporata":



Principio	Descrizione
Approccio preventivo e non reattivo	L'adozione di un **approccio preventivo e proattivo** piuttosto che reattivo e correttivo ha l'obiettivo di **anticipare e prevenire gli eventuali rischi** che possono ledere i diritti e le libertà degli interessati evitando così effetti negativi per i Dipartimenti e le Strutture Equiparate di Regione Calabria. L'obiettivo di un tale approccio, infatti, è quello di impedire che si verifichino violazioni della Privacy applicando i principi di Privacy by Design e by Default.
Approccio incentrato sull'interessato	L'adozione di un **approccio metodologico-strategico, che coinvolge attivamente l'interessato, ponendolo al centro del sistema** (approccio "*user-centric*"), consente di prevenire l'insorgenza di potenziali lesioni dei suoi diritti. Tale approccio, infatti, garantisce l'adozione di misure di protezione adeguate per impostazione predefinita e pone le basi affinché il trattamento sia lecito mediante l'applicazione delle basi giuridiche (art. 6 del GDPR).
Privacy incorporata nel design	Al fine di garantire un approccio proattivo, è necessario tutelare il dato sin dalla progettazione dei sistemi informatici e/o dei trattamenti. In tal modo, la **Privacy è incorporata nel disegno e nell'architettura dei nuovi sistemi e/o processi** e costituisce una componente essenziale ed integrante delle funzionalità principali. Il Titolare del trattamento dovrà pertanto essere in grado di adottare e attuare **misure tecniche e organizzative che tutelino i principi di protezione dei dati sin dal momento della progettazione oltre che in fase di esecuzione del trattamento**. In base al principio della Privacy by Design l'utente dovrà essere considerato al centro del sistema di Data Protection ogni qualvolta sia avviato un progetto, tenendo fin da subito in considerazione i suoi diritti e le sue libertà.
Privacy come impostazione predefinita	Per impostazione predefinita il Titolare dovrà trattare solo i Dati Personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Ciascun sistema di trattamento dovrà quindi essere definito garantendo la **minimizzazione dei dati** e la **limitazione delle finalità**. Il Titolare, in attuazione di tale principio dovrà, ad esempio, prevedere la protezione rafforzata di determinate informazioni all'interno dei sistemi informatici e prevedere delle impostazioni automatiche a maggior tutela dei dati dell'interessato. Il principio di Privacy by Default, pertanto, ha l'obiettivo di garantire il massimo grado di Privacy affinché gli interessati non debbano porre in essere ulteriori azioni per proteggere i loro dati personali, in quanto è integrata nei sistemi per impostazione predefinita.
Protezione completa	È necessario che i Dipartimenti e le Strutture Equiparate di Regione Calabria prevedano adeguate misure di sicurezza - essenziali per la Privacy - per tutto il ciclo di vita del dato, per garantire che tutti i dati siano opportunamente trattati, conservati e distrutti - in modo sicuro e tempestivo - alla fine del processo. La selezione delle misure di sicurezza da porre in essere dovrà essere commisurata alla rischiosità del trattamento. Il Titolare del trattamento dovrà pertanto essere in grado di adottare e attuare

	misure tecniche e organizzative che tutelino i principi di protezione dei dati sin dal momento della progettazione oltre che in fase di esecuzione del trattamento.

5.2 PRINCIPI OPERATIVI

Al fine di garantire la Privacy by Design e by Default, è opportuno conformarsi ai principi operativi volti ad orientare la progettazione, lo sviluppo e l'implementazione dei requisiti di protezione Privacy di seguito illustrati[1]:

Principio	Descrizione	Rischi
1. Base giuridica	Il Titolare del trattamento ha l'obbligo di valutare, prima di iniziare il trattamento, quale sia la base giuridica più idonea rispetto al trattamento che intende porre in essere. Ai sensi dell'art. 5 del GDPR che sancisce il principio di liceità, perché il trattamento di un Dato Personale sia lecito, deve fondarsi su una specifica base giuridica. Gli artt. 6, 9 e 10 del GDPR definiscono quando il trattamento può considerarsi lecito. Invero, i trattamenti afferenti ai Dipartimenti e alle Strutture Equiparate di Regione Calabria, trovano giustificazione in base a quanto stabilito dagli artt. 6, 9 e 10 del GDPR. In particolare, l'art. 6 del GDPR statuisce che il trattamento è lecito solo se ricorre una delle seguenti condizioni: a) consenso dell'interessato; b) esecuzione di un contratto o misure	In assenza di un'idonea base giuridica che autorizzi il trattamento dei Dati Personali possono verificarsi i seguenti rischi: • **l'Autorità di controllo**, in caso di violazione della normativa privacy, potrebbe **imporre al Titolare delle misure procedurali o tecniche di natura correttiva**, e imporre altresì la **limitazione, la sospensione e il blocco dei trattamenti**; • **minare il rapporto fiduciario intercorrente tra Titolare-interessato,** e generare possibili reazioni negative dell'interessato sia in forma diretta, sia tramite azioni che possono danneggiare la reputazione del Titolare. Infatti, il trattamento illegittimo dei Dati Personali comporta un danno alla reputazione e all'autorevolezza dell'Ente coinvolto. Ciò si riflette inevitabilmente anche sul rapporto che intercorre tra il Titolare ed eventuali contitolari; • **violare la normativa sulla protezione dei Dati Personali** vista l'assenza di una

[1] I principi di seguito illustrati si ispirano allo standard ISO/IEC 29100:2011 /Amd 1:2018 - "Information technology -- Security techniques -- Privacy framework"[4].

Principio	Descrizione	Rischi
	precontrattuali di cui l'interessato è parte; c) sussiste un obbligo legale in capo al Titolare del trattamento; d) salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica; e) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; f) perseguimento di un legittimo interesse del Titolare o di terzi, purché non prevalgano gli interessi o i diritti e le libertà dell'interessato. La base giuridica del legittimo interesse non si applica nell'ipotesi in cui il trattamento dei dati sia effettuato dalle Autorità Pubbliche nell'esecuzione dei loro compiti. L'art. 9 del GDPR illustra le condizioni che devono ricorrere affinché il Titolare possa trattare categorie particolari di dati, come dati relativi alla salute o alla vita sessuale dell'interessato. L'art. 10 del GDPR disciplina il trattamento dei dati afferenti alle condanne penali e reati. Tendenzialmente, le basi giuridiche maggiormente ricorrenti nei trattamenti realizzati dai Dipartimenti e dalle Strutture Equiparate di Regione Calabria sono: l'obbligo legale e l'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. **L'obbligo legale** prevede quattro presupposti, e dunque: • **adempimento di una legge europea o nazionale** dello Stato membro del soggetto Titolare; • le disposizioni di legge devono stabilire	base legale adeguata in virtù di quanto stabilito dagli artt. 6, 9 e 10 del GDPR; • **diminuire l'efficacia di alcune attività operative dei** Dipartimenti e delle Strutture Equiparate di Regione Calabria; • possibili **responsabilità legali con relative sanzioni:** gli interessati possono intraprendere azioni legali per danni derivanti dal trattamento illegittimo dei loro Dati Personali.

Principio	Descrizione	Rischi
	una necessità inconfutabile del trattamento dei Dati Personali sulla base di un **obbligo imperativo**; • la normativa di riferimento deve **definire le finalità** del trattamento in oggetto; • è rivolto al **Titolare** e non agli interessati. Per **l'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri,** i soggetti pubblici non sono tenuti a chiedere che l'interessato fornisca il suo consenso al trattamento dei suoi Dati Personali, dato che il trattamento sorge sulla base di quanto sancito all'interno di una norma europea o da disposizioni di legge dell'ordinamento interno che specificano le operazioni eseguibili e il **motivo di interesse pubblico rilevante**.	
2. Scopo legittimo e specifico	Il principio di legittimità e specificità dello scopo assicura che quest'ultimo sia conforme alla legge applicabile e si fondi su una base giuridica ammissibile.	I rischi potenziali sono numerosi e legati al fatto che vengono raccolti Dati Personali eccedenti rispetto a quelli strettamente necessari per soddisfare le finalità del trattamento. Il rischio è quello di esporre i Dipartimenti e le Strutture Equiparate di Regione Calabria ad un maggiore livello di responsabilità, a maggiori rischi afferenti alla sicurezza e ad una possibile violazione del principio della Data Protection by Default, nonché costi aggiuntivi di amministrazione dei dati. La mancata comunicazione delle finalità della raccolta dei dati all'interessato può minare il rapporto di fiducia che intercorre tra questi e il Titolare.
3. Limitazione della raccolta	Tale principio prevede la limitazione della raccolta dei Dati Personali a ciò che è	Un'eccessiva raccolta di dati può generare delle anomalie in fase di trattamento e

Principio	Descrizione	Rischi
	strettamente necessario per gli scopi specificati. I Dati Personali devono essere raccolti per finalità specifiche e legittime in linea con quanto dichiarato.	conservazione. **L'eccessiva raccolta di Dati Personali espone quindi i Dipartimenti e le Strutture Equiparate di Regione Calabria ad un maggiore costo di gestione e a maggiori responsabilità operative**. Maggiore è la quantità di Dati Personali raccolti, tanto maggiore è la probabilità che possano verificarsi degli errori, oppure che non venga rispettato il principio di accuratezza del dato. La raccolta di dati non trasparente o eccessiva può: • esporre Regione Calabria a **sanzioni a causa** dell'attuazione di pratiche operative ingannevoli; • creare **danni all'immagine di Regione Calabria** con una significativa reazione negativa da parte degli interessati, ove queste informazioni vengano pubblicizzate. Le considerazioni sopra illustrate si applicano non soltanto alle informazioni che vengono raccolte con metodi tradizionali, vale a dire su supporti cartacei, ma ancora di più si applicano alle informazioni raccolte mediante strumenti elettronici.
4. Minimizza-zione dei dati	Il principio della minimizzazione dei dati prevede la progettazione, l'implementazione e l'elaborazione dei dati, attraverso procedure o sistemi ICT, in modo da ridurre al minimo i Dati Personali che vengono elaborati e il numero di parti interessate.	Il trattamento e la comunicazione di Dati Personali eccedenti rispetto alle finalità definite in fase di raccolta possono: • **compromettere la fiducia degli interessati**; • far scaturire denunce per pratiche commerciali ingannevoli; • **generare il rischio che i Dati Personali vengano conservati oltre il periodo necessario per la finalità raccolta**, sostenendo quindi costi aggiuntivi di archiviazione.

Principio	Descrizione	Rischi
		Inoltre, in caso di mancata definizione della durata dei Dati Personali raccolti **è possibile che questi vengano distrutti in maniera prematura**, compromettendo la possibilità per gli interessati di accedere a tali dati limitandone la disponibilità. Le procedure di distruzione devono essere conformi alle vigenti normative europee, che costituiscono stato dell'arte per la procedura di distruzione.
5. Limitazione dell'utilizzo, conservazione e divulgazione	Tale principio prevede la limitazione dell'utilizzo, della conservazione e della divulgazione (incluso il trasferimento) dei Dati Personali rispetto a quanto è necessario per soddisfare gli scopi specifici, espliciti e legittimi del trattamento.	La mancata limitazione dell'utilizzo, conservazione e divulgazione comporta: • il rischio che i dati vengano **utilizzati** per **scopi diversi** da quelli prestabiliti; • il rischio che i Dati Personali raccolti vengano conservati **oltre il periodo necessario** per la finalità indicata, e che non vengano anonimizzati correttamente.
6. Precisione e qualità	Il principio di accuratezza e qualità assicura che i Dati Personali elaborati siano accurati, completi, aggiornati (a meno che non vi sia una base legittima per mantenere dati obsoleti), adeguati e pertinenti alle finalità del trattamento.	L'utilizzo di dati non accurati, al fine di prendere decisioni afferenti agli interessati, può portare a **perdite di profitti.** Infatti, Dati Personali non accurati possono danneggiare gli interessati e compromettere la relazione con lo stesso. I Dipartimenti e le Strutture Equiparate di Regione Calabria devono pertanto **identificare i criteri di aggiornamento dei dati**, al fine di **evitare una dispersione di risorse** per aggiornamenti non necessari.
7. Apertura, trasparenza e preavviso	Tale principio prevede di fornire **informazioni chiare e facilmente accessibili** sulle politiche stabilite dal Titolare del trattamento e sulle procedure e pratiche relative al trattamento dei Dati Personali.	La mancata trasparenza nel comportamento adottato dal Titolare potrebbe avere i seguenti impatti: • **impedire agli interessati di comprendere a fondo come i Dipartimenti e le Strutture Equiparate di Regione Calabria trattano e**

Principio	Descrizione	Rischi
		proteggono i Dati Personali affidati dall'interessato stesso; • diminuire la **possibilità di ottenere un consenso** al trattamento stesso; • **ridurre il livello di fiducia dell'interessato**. Parimenti, la mancanza di trasparenza può far sì che l'interessato possa rendersi conto del fatto che alcuni dati possono essere comunicati a terzi, creando potenziali disguidi e malintesi, che influenzano negativamente l'immagine di Regione Calabria.
8. Partecipazione individuale e accesso	Il principio della partecipazione e dell'accesso individuale prevede di fornire agli interessati la **possibilità di accedere e di rivedere i propri Dati Personali**, a condizione che la loro identità sia autenticata con un livello adeguato di garanzia e che l'accesso non sia vietato dalla legge.	La mancata elaborazione ed attuazione di una procedura per la gestione dei diritti di accesso dell'interessato può portare ad un **trattamento di Dati Personali non corretto o aggiornato**. Il mancato rispetto, entro limiti temporali ben definiti, di una richiesta di accesso a Dati Personali può portare all'applicazione di **significative sanzioni**.
9. Responsabiliz-zazione	Il principio dell'accountability prevede di documentare e comunicare in modo appropriato tutte le politiche, le procedure e le pratiche adottate nell'ambito della Data Protection. Prevede, altresì, l'assegnazione al Delegato del Titolare del compito di attuare le politiche, le procedure e le best practices in materia di protezione dei dati all'interno di ciascuno dei Dipartimenti e delle Strutture Equiparate di Regione Calabria.	In materia di responsabilizzazione, il rischio associato potrebbe comportare ad esempio: • rivelazione **non autorizzata di Dati Personali;** • **trattamenti non consentiti o illeciti**; • **danno all'immagine;** • **difficoltà di gestione delle richieste** degli interessati; • **risarcimento del danno;** • sanzioni.
10. Sicurezza delle informazioni	Il principio di sicurezza delle informazioni prevede la protezione dei Dati Personali sotto la propria responsabilità con dei controlli appropriati a livello operativo, funzionale e strategico. **L'obiettivo è quello di garantire l'integrità, la riservatezza e la disponibilità dei Dati Personali** e proteggerli dai rischi, quali l'accesso non autorizzato, la	Il mancato utilizzo di appropriati meccanismi di controllo di accesso comporta il rischio che **soggetti terzi non autorizzati possano accedere ai Dati Personali** e utilizzarli per finalità non previamente autorizzate. Tali azioni possono creare un danno

Principio	Descrizione	Rischi
	distruzione, l'utilizzo non consentito, la modifica, la divulgazione o la perdita durante tutto il ciclo di vita del trattamento del dato.	significativo all'interessato ed essere fonte di responsabilità.
11. Conformità alla normativa	Il principio della conformità alla normativa prevede di verificare e dimostrare che il trattamento rispetti la protezione dei dati e la tutela della Privacy, attraverso requisiti specifici e mediante **verifiche periodiche** - anche attraverso il ricorso a revisori interni o esterni.	Se non si ha a disposizione un efficiente sistema di verifica della conformità del trattamento alle disposizioni regolamentari, potrebbe essere difficile determinare: • **il rispetto dei dettami in materia di raccolta**, trattamento, comunicazione e conservazione dei Dati Personali; • **problemi di natura legale**, che potrebbero portare all'applicazione di significative sanzioni; • **riflessi negativi sulla qualità e continuità delle attività organizzate.**
12. Gestione dei Data Breach	L'obiettivo dell'articolo 33 del GDPR è quello di porre tempestivo riparo alle conseguenze, potenzialmente gravi, di una **violazione di Dati Personali** (c.d. "Data Breach"). Gli artt. 33 e 34 del GDPR stabiliscono che la notifica all'Autorità di controllo o la comunicazione all'interessato debba essere effettuata, senza ingiustificato ritardo, nell'ipotesi in cui la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Le conseguenze della violazione di dati personali possono essere estremamente diversificate, in funzione del fatto che la violazione comporti la perdita di un dato, piuttosto che la sottrazione ed il possibile utilizzo abusivo da parte di chi ha sottratto il dato. La metodologia adottata da Regione Calabria, con Decreto Dirigenziale n°. 2349	La mancata o inadeguata gestione delle violazioni di Dati Personali comporta la **non conformità alla normativa**. Pertanto, è di estrema rilevanza la conformità alla normativa dettata e a quanto stabilito dalla Procedura di gestione Data Breach[12] adottata da Regione Calabria, che sancisce le modalità e le tempistiche di azione, in caso di violazione dei dati, al fine di non incorrere in importanti sanzioni.

Principio	Descrizione	Rischi
	del 09 marzo 2021 “Approvazione processo di gestione Data Breach (incidenti di sicurezza dati Regione Calabria)”[12], **prevede tre parametri per valutare la gravità dell’evento**. In particolare, si valuta: - **il volume dei dati violati**; - **la tipologia dei dati violati**; - **l’impatto della violazione**. Valutata la gravità della violazione, il processo consta di varie fasi: - **segnalazione**: tutti gli eventi che potrebbero presentare dei rischi di Data Breach devono essere immediatamente segnalati; - **archiviazione**: le segnalazioni, le eventuali misure adottate e le comunicazioni effettuate devono essere archiviate; - **valutazione e misure**: accertata la violazione devono determinarsi le misure di contenimento e di contrasto per arginare la violazione; - **notifica all’Autorità Garante, ove necessario**.	
13. Trasferimento dati all'estero	I Dati Personali possono essere trasferiti anche al di fuori dell’Unione Europea, in paesi terzi, a condizione che tali paesi siano stati sottoposti a una valutazione di idoneità delle disposizioni di legge, ivi esistenti ed afferenti alla protezione dei Dati Personali e che siano implementate garanzie adeguate.	I rischi potenziali sono principalmente: • rischi legati al fatto che il paese terzo in questione **non garantisce una sufficiente protezione dei Dati Personali**; • rischi legati al fatto che l’introduzione di eventuali **regole e leggi cogenti**, che permettono di trasferire Dati Personali in paesi terzi, **non siano rispettate.** Il verificarsi di entrambi i rischi può portare a conseguenze estremamente gravi, in termini di applicazione di sanzioni, che possono raggiungere importi elevati.

6. LE MISURE DI SICUREZZA ICT

La Regione Calabria, al fine di prevenire e reagire ad incidenti cibernetici e con l'obiettivo di contrastare le minacce informatiche più frequenti, ha attuato quanto previsto da AgID nella circolare n. 2/2017 del 18 Aprile 2017 recante: "Misure minime di sicurezza ICT per le pubbliche amministrazioni", in attuazione della direttiva del Presidente del Consiglio dei Ministri del 1° agosto 2015.

In tal senso, i Dipartimenti e le Strutture Equiparate di Regione Calabria nell'ambito di ogni nuovo progetto/ trattamento/processo, sin dalle prime fasi di progettazione, devono attenersi alle misure di sicurezza obbligatorie già implementate da Regione Calabria, in considerazione dei documenti di "Analisi della compliance rispetto alle misure di sicurezza obbligatorie AgID"[8] e del relativo "Modulo di implementazione delle Misure Minime di Sicurezza ICT di Regione Calabria" del 1° Settembre 2021[9]. Nei presenti documenti, sono identificate le modalità di implementazione presso l'Ente delle 8 classi di controllo ABSC (AgID Basic Security Controls). Questo approccio si basa sull'identificazione dei possibili scenari di rischio che potrebbero verificarsi, infatti, in base ai rischi valutati le misure di sicurezza possono presentare tre livelli di rischio[2]: alto, medio e basso. Tale metodo di analisi del rischio, in linea con quanto disciplinato dal GDPR all'art. 32, consente di mettere da subito in campo le misure preventive più efficaci e ridurre al minimo gli interventi correttivi successivi.

Di seguito sono illustrate le modalità di implementazione nel contesto della Regione Calabria, per ogni controllo AgID:

Misura minima ABSC AgID	**Modalità di implementazione**
ABSC-01 Inventario dei dispositivi autorizzati e non autorizzati	Il Presidio Sistemi di Regione Calabria, con il coordinamento dei dipartimenti/strutture dell'Ente, provvede ad alimentare l'inventario dei dispositivi hardware che sono in grado di memorizzare o elaborare dati (*risorse attive*), nel Tool che gestisce l'Asset Inventory[3]. Al contempo, provvede opportunamente ad aggiornare l'inventario con i dispositivi hardware abilitati al collegamento in rete, registrando altresì l'indirizzo IP, in aggiunta ai dati identificativi presi in considerazione per il censimento delle risorse attive. Dunque, Regione Calabria provvede a mantenere un inventario aggiornato di tutti i dispositivi autorizzati alla connessione, riducendo dunque il rischio

[2] Per maggiori informazioni sul processo di Privacy by Design e By Default si rimanda al "Decreto Dirigenziale di Regione Calabria n. 10388 del 14 ottobre 2021 "Approvazione del processo di gestione della Privacy by Design e by Default per la Regione Calabria".

[3] Le specifiche sono definite nei documenti di "Politica Asset Management" e "Procedura Asset Inventory" formalizzate in data 18 aprile 2024 nell'ambito del progetto "Rafforzamento della Cybersicurezza e della Data Protection dei Sistemi e dei processi connessi all'erogazione dei servizi della Regione Calabria alle ASP e AO regionali".

Misura minima ABSC AgID	Modalità di implementazione
	di accessi non autorizzati, al fine di garantire la corretta protezione dei dati dell'Ente.
ABSC-02 Inventario dei software autorizzati e non autorizzati	Regione Calabria provvede al censimento dell'elenco dei software, che possono essere installati ed impiegati dal personale dell'ente, attraverso il Tool di Asset Inventory. A tal proposito, viene negata la possibilità agli utenti delle postazioni di lavoro in dominio *regcal*, di utilizzare applicativi/piattaforme/tool ecc. non compresi nell'elenco e dunque di software non autorizzati.
ABSC-03 La protezione delle configurazioni hardware e software sui dispostivi mobili, laptop, workstation e server	Regione Calabria attua un preciso meccanismo di protezione delle configurazioni hardware e software sui dispositivi mobili, laptop, workstation e server in uso dall'ente. In tal senso, il software di base utilizzato per le postazioni in dominio *regcal,* rispetta le configurazioni sicure *standard* sia per la tutela del sistema operativo installato che per i diversi sistemi IT utilizzati al fine di impedire che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.
ABSC-04 Valutazione e correzione continua delle vulnerabilità	Al fine di individuare le vulnerabilità e di correggere e minimizzare la possibilità di subire attacchi informatici, si compie una costante analisi dei sistemi in uso. Tale operazione risulta necessaria per verificare tempestivamente le vulnerabilità dei sistemi, adottando preventivamente un aggiornamento automatico, per i sistemi connessi alla rete, e ricorrente per quelli separati dalla rete, con l'ausilio di misure adeguate al livello di criticità emerso. La ricerca delle vulnerabilità sulle risorse IT è svolta dall'Ente attraverso l'applicativo FortiAnalyzer (Fortinet) che riporta e risolve tutte le vulnerabilità rilevate sulle risorse esaminate. Inoltre, Regione Calabria attua un piano di gestione dei rischi che tenga conto dei livelli di severità delle vulnerabilità, del potenziale impatto sull'Ente e della probabilità di subire attacchi sulla base della tipologia della risorsa IT.
ABSC-05 Uso appropriato dei privilegi amministrativi	Gli Amministratori di Sistema, quali utenti privilegiati, autorizzati alla gestione di specifici sistemi/piattaforme/applicativi ecc., sono selezionati sulla base delle proprie competenze, mediante apposita lettera di designazione che definisce altresì l'ambito di operatività degli stessi. Regione Calabria, nell'ambito del progetto di "Governo della Cybersecurity e della Data Protection", ha definito una procedura dettagliata in data 02 maggio 2024 per la corretta governance degli Amministratori di Sistema rivolta a tutti i Dipartimenti e le Strutture Equiparate di Regione Calabria. La procedura identifica, in maniera chiara, i ruoli e le responsabilità degli Amministratori di Sistema in virtù di quanto stabilito dalle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti

Misura minima ABSC AgID	Modalità di implementazione
	elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27 novembre 2008 e ss.mm.ii. e delle relative FAQ del Garante della Protezione dei Dati Personali. Inoltre, tutti gli accessi relativi agli Amministratori di Sistema sono registrati utilizzando soluzioni differenti rispetto all'ambito dei sistemi coinvolti (es. Graylog Log Management, Fortinet FortiAnalyzer, etc.). Il Registro degli Amministratori di Sistema, con le informazioni relative a ciascun amministratore, è situato nella share di rete "Misure Minime Sicurezza AGID\01 Amministratori Sistema". Le utenze amministrative sono gestite attraverso un apposito sistema di gestione delle identità, Red Hat FreeIPA, al fine di garantire la tempestiva disponibilità delle utenze in caso di emergenza.
ABSC-08 Le difese contro i malware	Sui dispositivi in dotazione dall'Ente sono installati, e costantemente aggiornati in modo automatico, i sistemi di protezione quali il firewall FortiGate (Fortinet) e l'antivirus, capaci di rilevare, segnalare e direttamente contrastare potenziali attacchi malware. Tali sistemi di protezione agiscono altresì al fine di filtrare, e conseguentemente bloccare, i contenuti potenzialmente nocivi della navigazione in rete e/o dei messaggi di posta elettronica. La garanzia di difesa contro i malware è attuata anche limitando l'uso di PC esterni, consentito solo previa autorizzazione della Regione Calabria, o di dispositivi di archiviazione esterni, i quali devono dotarsi di sistemi di crittografia. I software utilizzati per la protezione dai malware variano a seconda della tipologia di minacce esterne: - Apache SpamAssassin, utilizzato per filtrare la posta elettronica e bloccare eventuali contenuti nocivi - Next-generation Fortinet FortiGate, utilizzato per filtrare il traffico web e bloccare eventuali contenuti nocivi.
ABSC-10 Copie di sicurezza	La salvaguardia delle copie di sicurezze delle informazioni critiche è garantita dalla definizione di apposite procedure di esecuzione e dall'ausilio di determinati strumenti. Regione Calabria dispone la realizzazione di backup cifrati con cadenza mediamente giornaliera, su supporti fisici e in cloud, che assicurano il ripristino dei dati in caso di incidenti informatici.
ABSC-13 La Protezione dei	Poiché sono trattati dati identificabili come strettamente confidenziali (es.

Misura minima ABSC AgID	Modalità di implementazione
dati	dati personali particolari o dati giudiziari), questi richiedono una protezione adeguata, qual è la crittografia, con l'obiettivo di tutelare la loro integrità e pertanto eludere l'esfiltrazione degli stessi. Inoltre, la navigazione in rete deve essere limitata impedendo l'accesso a determinati siti web al fine di proteggere l'Ente da qualsiasi potenziale malware o plugin non sicuro, o più in generale da minacce di sicurezza.

Inoltre, per quanto concerne le ulteriori misure minime ENISA (cfr. Manuale ENISA sulla Sicurezza nel trattamento dei dati personali, dicembre 2017 normativa ENISA) si rimanda a quanto previsto nel documento di "Metodologia di valutazione d'impatto per la protezione dei dati personali (DPIA) per la Regione Calabria" del 23 marzo 2021 approvata con Decreto Dirigenziale n. 6786 del 30 giugno 2021[6].

In conclusione, sulla base dei principi generali illustrati e delle misure di sicurezze ICT implementate, l'approccio "**Privacy Embedded**" ossia di "Privacy incorporata" deve ripercorrere ciascuna fase del **ciclo di vita di sviluppo di un sistema e/o di un trattamento**, sin dalla fase di progettazione, prevedendo una serie di attività specifiche per garantire l'adozione di misure tecniche e organizzative adeguate alla protezione dei diritti e delle libertà degli interessati.

In tal senso, al fine di comprendere il processo di gestione di Privacy By Design e By Default adottato dalla Regione Calabria, come già specificato al par. 1.2, si rimanda a ciò che è stato approvato con Decreto Dirigenziale n. 10388 del 14 ottobre 2021[7], nel quale sono descritte le attività da compiere ed altresì sono individuate le figure che detengono i ruoli di responsabilità, sulla base della ripartizione delle competenze in materia di gestione dei diritti degli interessati previste Regolamento Regionale n. 20 del 18 dicembre 2018, modificato dalla Deliberazione di Giunta Regionale n. 29 del 1° febbraio 2021[5], oltre a specificare la strumentazione a supporto.

6.1 LE NUOVE MISURE INTRODOTTE DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN)

Con Decreto Legge n.82 del 14 giugno 2021 è stata istituita l'Agenzia per la cybersicurezza nazionale (ACN) che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Tra i suoi compiti: la tutela degli interessi nazionali nel campo della cybersicurezza, tutelare la sicurezza e la resilienza nello spazio cibernetico, prevenendo e mitigando il maggior numero di attacchi cibernetici nonché favorire l'autonomia tecnologica.

Il 17 maggio 2024 è stata attuata la Strategia Nazionale di Cybersicurezza di ACN e l'annesso Piano di implementazione, che contengono gli obiettivi di sicurezza da perseguire sia dalle Pubbliche Amministrazioni

che dai privati entro il 2026. Il fine della Strategia è la promozione di un approccio di sicurezza basato sul rischio e la resilienza delle infrastrutture critiche mediante l'adozione di 82 "misure adeguate" e proporzionate alla criticità dei sistemi[4].

Inoltre, ACN d'intesa con il Dipartimento per la trasformazione digitale, ha adottato **"il Regolamento per le infrastrutture digitali e per i servizi cloud per la PA"** che consentirà di guidare le Pubbliche Amministrazioni nella transizione sicura al cloud[5].

L'obiettivo che l'Agenzia vuole pervenire con questo provvedimento è quello di definire, in un unico quadro normativo, le misure minime che le infrastrutture come i data center e i servizi cloud devono rispettare per supportare i servizi pubblici.

Il regolamento (adottato con Decreto Direttoriale n. 21007/24, ai sensi dell'articolo 33-septies, comma 4, del Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221) si rivolge sia alle Pubbliche Amministrazione che ai fornitori di servizi cloud e abroga il precedente Regolamento adottato il 15 dicembre 2021 con Delibera n. 628/2021 dell'Agenzia per l'Italia Digitale.

[4] Strategia nazionale di cybersicurezza 2022-2026 predisposta dall'Agenzia per la cybersicurezza nazionale e adottata dal Presidente del Consiglio – 17 maggio 2024. Si riporta di seguito il link: https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza.

[5] Regolamento per le infrastrutture digitali e per i servizi cloud per la PA adottato da ACN con Decreto Direttoriale n. 21007/24, ai sensi dell'articolo 33-septies, comma 4, del Decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221. Si riporta di seguito il link: https://www.acn.gov.it/portale/cloud/regolamento-cloud-per-la-pa .