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

Revisione / aggiornamento procedura di gestione Data Breach

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		
	Alfredo Mazzitelli (Ntt Data Italia S.p.A.), Referente Servizi Adeguamento Organizzativo - GDPR e MM AgID	
Verifica		
	Gennaro Oriolo (Leonardo S.p.A.), Responsabile Tecnico Erogazione Servizi	
Approvazione		
Autorizzazione		

1 INTRODUZIONE

Il 24 maggio 2016 è entrato in vigore il *"Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio 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 (GDPR) e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*. A partire dal 25 maggio 2018 questo regolamento è pienamente applicabile in tutti gli Stati membri. Elemento cardine di questa normativa è il concetto di *"accountability"* con il quale viene introdotta la responsabilizzazione dei soggetti coinvolti nella protezione dei dati personali e la capacità di rendere conto delle proprie azioni.

Una delle novità introdotte dal GDPR è costituita dal *processo di gestione dei Data Breach* attraverso cui viene indicato il processo di gestione degli eventi di violazione dei dati personali comprendendo l'eventuale contatto tra titolare e autorità garante e tra titolare e interessato nel caso di violazione. Il presente documento descrive il processo che Regione Calabria ha adottato per gestire gli eventi anomali e gli incidenti di violazione dei dati personali. Nella stesura si è tenuto conto di quanto previsto nella normativa di riferimento pur essendo soggetta ad aggiornamenti futuri dovuti ad interventi chiarificatori da parte del Garante della Privacy.

Rif.	Codice	Titolo
DR-1.	GDPR 2016/679	Regolamento UE n. 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).
DR-2.	WP250	WP250, rev.01 "Linee-guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" - Gruppo di lavoro Articolo 29 per la protezione dei Dati.
DR-3.	D.L. 101/2018	DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" - G.U. 4 settembre 2018 n.205.

Tabella 1: Documenti di riferimento

2 DEFINIZIONI E ACRONIMI

2.1 Definizioni

Termine	Descrizione
Anonimizzazione	Tecnica che viene applicata ai dati personali in modo tale che le persone fisiche interessate non possano più essere identificate in nessun modo.
Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.
Cifratura	Processo che rende un determinato dato personale non decifrabile a soggetti non autorizzati.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Data Breach	Una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Termine	Descrizione
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
Interessato	La persona fisica identificata o identificabile cui si riferiscono i dati personali. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Misure di sicurezza	Insieme di misure sia tecniche che organizzative in grado di garantire un livello di sicurezza dei dati trattati adeguato al rischio.
Privacy by Design / by Default	Approccio concettuale che impone l'obbligo di prevedere fin da subito gli strumenti e le corrette impostazioni a tutela dei dati personali.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione	Il trattamento dei dati personali effettuato in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Termine	Descrizione
Titolare del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Tabella 2: Definizioni

2.2 Acronimi e riferimenti

Termine	Descrizione
DPIA (o PIA)	Data Protection Impact Assessment (o Privacy Impact Assessment). È una procedura prevista dall'articolo 35 del GDPR che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.
RPD (o DPO)	Responsabile della Protezione dei Dati Personali (Data Protection Officer)
GDPR	General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati) 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
Delegato del Titolare	Riferimento al "Delegato al trattamento dei dati personali"
Settore Agenda Digitale	Riferimento al settore "ICT, E-Governement e Agenda Digitale" del Dipartimento "Presidenza"
Settore Datore di Lavoro	Riferimento al settore "Datore di lavoro, sicurezza luoghi di lavoro, privacy-Rapporti con gli Enti Locali e Polizia Locale" del Dipartimento "Organizzazione e risorse umane"

Tabella 3: Acronimi e riferimenti

3 QUADRO NORMATIVO

Gli articoli del Regolamento UE n. 2016/679 che normano l'ambito di applicazione del presente documento sono:

- art. 4 par. 12 che definisce la violazione dei dati personali;
- art. 33 e art. 34 che elencano gli adempimenti previsti in caso di violazione.

3.1 Definizione di Violazione dei dati personali

L'art. 4 par. 12 del GDPR definisce la "violazione dei dati personali" (Data Breach) come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

3.2 Notifica di una violazione dei dati personali all'autorità di controllo

L'art. 33 del GDPR indica gli adempimenti previsti dalla normativa in caso di violazione dei dati personali relativamente alla notifica da inviare all'autorità di controllo.

Articolo 33 - "Notifica di una violazione dei dati personali all'autorità di controllo"

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3.La notifica di cui al paragrafo 1 deve almeno:

> *a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*
>
> *b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
>
> *c) descrivere le probabili conseguenze della violazione dei dati personali;*
>
> *d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

4.Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5.Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

3.3 Comunicazione di una violazione dei dati personali all'interessato

L'art. 34 del GDPR indica gli adempimenti previsti dalla normativa in caso di violazione dei dati personali relativamente alla comunicazione da inviare all'interessato.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1.Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. 4.5.2016 L 119/52 Gazzetta ufficiale dell'Unione europea IT

2.La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3.Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

> *a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
>
> *b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;*
>
> *c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

4.Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

In definitiva, in base agli art. 33 e 34 del GDPR, i Titolari dei trattamenti hanno in carico:

1) la notifica all'autorità di controllo delle violazioni riscontrate entro 72 ore e comunque "senza ingiustificato ritardo" (art. 33). Tale comunicazione non è obbligatoria se i Titolari ritengono improbabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

2) la comunicazione all'interessato, "senza ingiustificato ritardo", della violazione dei dati personali (art. 34) quando la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche. Se sono rispettate le condizioni riportate all'art. 34 par. 3 tale comunicazione non è obbligatoria.

Inoltre, il Titolare deve istituire un registro che contenga tutte le violazioni riscontrate e tutte le informazioni reperite durante l'analisi del singolo evento.

4 TASSONOMIA DEGLI EVENTI

Le linee guida descritte nel documento si applicano a tutti gli archivi cartacei e a tutti i sistemi informatici regionali in cui sono conservati i dati personali degli interessati intesi come cittadini, dipendenti, fornitori. Di seguito viene riportato un elenco non esaustivo di eventi che possono determinare una violazione di dati personali. Il verificarsi di uno degli eventi indicati non sempre implica l'effettiva sussistenza di un data breach ma serve ad allertare il team di valutazione per stabilire, tramite un'analisi approfondita, la fondatezza o meno della violazione. Nei paragrafi successivi gli eventi vengono classificati in base alla tipologia di trattamento (elettronico o cartaceo) e, per ogni tipologia, si riportano esempi di eventi suddivisi in due macro aree: accidentale (evento determinato da cause fortuite) o doloso (evento causato da personale consapevole del danno procurato).

4.1 Trattamenti elettronici

4.1.1 Eventi accidentali

Evento	Esempi
Esecuzione erronea di comandi e/o procedure	• pubblicazione erronea delle informazioni personali (non di dominio pubblico) su siti web dell'Amministrazione regionale; • erroneo invio di informazioni a enti/soggetti esterni all'Amministrazione regionale; • formattazione di dispositivi di memorizzazione; • errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; • divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato.
Rottura di componenti hardware	• distruzione di supporti di memorizzazione a causa di caduta accidentale, eventi atmosferici, incendi, sbalzi di elettricità, o corto circuito.
Malfunzionamento di software	• esecuzione di uno script automatico non autorizzato; • errori di programmazione del software che causano output errati.
Visibilità errata di dati sui siti web dell'Amministrazione	• visibilità da parte di utenti di dati di altri utenti.
Fornitura di dati a persona diversa dall'interessato	• comunicazioni di dati di interessati a destinatari errati; • gestione di informazioni richieste da persone diverse dal Titolare o suo delegato.

Guasti alla rete	• caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione.

Tabella 4: Trattamenti elettronici: eventi accidentali

4.1.2 Eventi dolosi

Evento	Esempi
Furto	• furto di supporti di memorizzazione e/o elaborazione contenenti dati personali.
Truffa informatica esterna	• frode realizzata da un soggetto esterno all'Amministrazione che causa perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori, mediante: ○ accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi; ○ appropriazione di dati bancari; ○ appropriazione (e diffusione) delle credenziali di autenticazione ai servizi degli utenti.
Truffa informatica interna	• frode realizzata da personale interno all'Amministrazione che comporta la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

Tabella 5: Trattamenti elettronici: eventi dolosi

4.2 Trattamenti cartacei

4.2.1 Eventi accidentali

Evento	Esempi
Distruzione accidentale di documenti	• distruzione di documenti causata da incendio/allagamento dei locali dove sono presenti gli archivi cartacei presso le sedi della Regione e/o Enti collegati o di propri fornitori; • distruzione per errore di documenti originali, senza eventuale copia.
Smarrimento di documenti	• perdita di documenti contenenti dati personali.
Fornitura involontaria di dati a persona diversa dal contraente	• invio lettera ad ente senza mandato; • invio/visualizzazione di fatture a soggetti

	diversi dal titolare della linea; • gestione/evasione richieste di informazioni avanzate da persone diverse dal titolare della linea non delegato.

Tabella 6: Trattamenti cartacei: eventi accidentali

4.2.2 Eventi dolosi

Evento	Esempi
Distruzione dolosa dei documenti	• incendio doloso provocato da personale interno o esterno che rende indisponibile in modo definitivo i documenti contenenti dati personali; • accesso non autorizzato da parte di terzi ad archivi interni dell'Amministrazione e distruzione volontaria di documenti contenenti dati personali.
Accesso non autorizzato	• accesso non autorizzato da parte di personale interno o esterno, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi della Regione e/o Enti o propri fornitori. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
Furto	• sottrazione da parte di personale interno o esterno (o non identificati) di documenti cartacei contenenti dati personali.

Tabella 7: Trattamenti cartacei: eventi dolosi

5 GRAVITA' DELL'EVENTO

Il GDPR con l'art. 33 e l'art. 34 stabilisce che la notifica all'autorità di controllo o la comunicazione all'interessato debba essere effettuata qualora la violazione dei dati personali presenti un rischio (o rischio elevato nel caso di comunicazione all'interessato) per i diritti e le libertà delle persone fisiche. Fatte salve le casistiche di esclusione della notifica, resta a carico del titolare la valutazione della gravità connesso alla violazione. Il Regolamento europea, in base al principio di responsabilizzazione, non specifica un metodo di valutazione lasciando al titolare piena autonomia nella scelta dell'approccio da seguire. Nel paragrafo successivo viene proposta una metodologia per la valutazione della gravità dell'evento derivata da quella utilizzata dall'autorità garante spagnola AEPD (Agencia Española de Protección de Datos).

5.1 Metodologia di valutazione

La presente metodologia valuta la gravità dell'evento, mediante la combinazione di tre parametri di valutazione, e suggerisce al Titolare del trattamento le relative azioni da intraprendere. Le possibili azioni da intraprendere consistono nella notificazione dell'evento all'autorità garante o la comunicazione specifica agli interessati.

I tre parametri sono:

- Volume dei dati violati;
- Tipologia dei dati violati;
- Impatto della violazione.

Questi parametri sono valutati mediante l'attribuzione di un punteggio che segue i criteri descritti nella tabella successiva:

VOLUME DEI DATI VIOLATI	
Numero di record di identificazione completi	***Punteggio***
Meno di 100	1
Tra 100 e 1.000	2
Tra 1.000 e 100.000	3
Tra 100.000 a 1.000.000	4
Oltre 1.000.000	5

TIPOLOGIA DEI DATI VIOLATI	
Tipologia di dato personale	***Punteggio***
Dato personale comune	1
Dato particolare / giudiziario	2

IMPATTO DELLA VIOLAZIONE	
Grado di divulgazione	***Punteggio***
Nessuna divulgazione	2
Interna all'Ente, controllata	4
Esterna all'Ente	6
Pubblica (es. divulgazione su Internet)	8
Sconosciuta	10

Tabella 8: Parametri metodologia

La gravità potenziale è data dalla seguente formula:

$$Gravità\,\% = Volume * Tipologia * Impatto$$

Ottenuta la gravità potenziale della violazione, si forniscono due regole per stabilire quando inviare la notifica o la comunicazione:

1) Occorre inviare la **notifica all'autorità garante** se sono soddisfatti contemporaneamente questi due criteri:
    a. Il valore del rischio è uguale o superiore a 20%, e
    b. Almeno due dei tre parametri hanno un valore compreso tra quelli evidenziati in azzurro.
2) Occorre inviare la **comunicazione all'interessato** se sono soddisfatti contemporaneamente questi due criteri:
    a. Il valore del rischio è uguale o superiore a 40%, e
    b. Almeno due dei tre parametri hanno un valore compreso tra quelli evidenziati in azzurro.

5.2 Esempio di applicazione metodologia

La classificazione e l'analisi di un esempio di violazione di dati personali può essere riassunta dalla tabella seguente:

CLASSIFICAZIONE	
Tipo di violazione	Riservatezza
Tassonomia	Accesso ad account con privilegi avanzati
Origine della minaccia	Esterna
Gravità	Alta

ANALISI			
Volume dei dati	500 record	>>	2
Tipi di dati	Dati personali particolari	>>	2
Impatto	Divulgazione pubblica	>>	8

Tabella 9: Esempio metodologia

Applicando la formula presente al par. 6.1, otteniamo:

$$Gravità\,\% = Volume * Tipologia * Impatto = 2 * 2 * 8 = 32\,\%$$

Nel caso in esame, due parametri hanno valori compresi tra quelli evidenziati in azzurro e il valore della gravità è pari a 32% per cui, la metodologia fornisce al Titolare l'indicazione dell'invio della sola notifica al Garante.

6 PROCESSO DI GESTIONE DI EVENTI ANOMALI / INCIDENTI

La presente sezione riporta i ruoli e le strutture coinvolti con i relativi compiti e la rappresentazione grafica del processo di gestione degli eventi di possibile violazione dei dati Personali.

6.1 Ruoli e strutture coinvolti nel processo

In questo paragrafo, sono elencate le strutture e i ruoli coinvolti nel processo di gestione dei Data Breach. A partire dalla segnalazione di un possibile evento di violazione dei dati personali, che può essere comunicato in qualsiasi modo da un soggetto esterno o interno all'amministrazione, sono stati assegnati compiti specifici ad ogni figura o struttura.

- *Delegato del Titolare*:
    - inoltra al "Settore Agenda Digitale", al "Settore Datore di Lavoro" e al RPD qualsiasi informazione acquisita su eventi anomali o violazioni di sicurezza sui dati personali, per ottenere supporto nelle attività di valutazione della gravità di eventuali violazioni di sicurezza e nelle attività di determinazione delle relative misure di contenimento e contrasto per porre rimedio a tali violazioni;

- in caso di violazione di dati personali che comporti un rischio non trascurabile per i diritti e le libertà delle persone fisiche, notifica la violazione al Garante Privacy nei tempi e con le modalità di cui all'art. 33 del GDPR, con il supporto del Settore Datore di Lavoro e del RPD;
- in caso di violazione di dati personali che comporti un rischio molto alto per i diritti e le libertà delle persone fisiche, comunica la violazione agli interessati nei tempi e con le modalità di cui all'art. 34 del GDPR, con il supporto del Settore Datore di Lavoro e del RPD.

- *Settore Agenda Digitale*:
  - predispone, tiene e aggiorna il "*Registro regionale degli incidenti sui dati personali*" per tracciare e documentare gli eventi anomali e le violazioni sui dati personali trattati;
  - supporta i delegati del Titolare del trattamento, con la collaborazione del Settore Datore di Lavoro, nelle attività di valutazione della gravità di eventuali violazioni di sicurezza e nelle attività di determinazione delle relative misure di contenimento e contrasto per porre rimedio a tali violazioni;
  - attiva le strutture preposte all'attuazione delle misure di contenimento e contrasto. Il gruppo delle strutture attivate costituisce l'*Incident Response Team*;
  - collabora con il Settore Datore di Lavoro, nella predisposizione delle notifiche di violazioni di dati personali al Garante Privacy;
  - collabora con il Settore Datore di Lavoro, nella predisposizione delle comunicazioni di violazioni di dati personali agli interessati.

- *Settore Datore di Lavoro*:
  - collabora con il Settore Agenda Digitale nelle attività di valutazione della gravità di eventuali data breach e nelle attività di determinazione delle relative misure di contenimento e contrasto per porre rimedio a tali violazioni, in particolar modo per quanto riguarda le violazioni di sicurezza sui trattamenti cartacei;
  - supporta i delegati del Titolare del trattamento, con la collaborazione del Settore Agenda Digitale, nella predisposizione delle notifiche di violazioni di dati personali al Garante Privacy;
  - supporta i delegati del Titolare del trattamento, con la collaborazione del Settore Agenda Digitale, nella predisposizione delle comunicazioni di violazioni di dati personali agli interessati.
- *RPD*: fornisce supporto durante la fase di notifica degli incidenti di sicurezza;

- *Responsabile del trattamento*: nell'ambito del servizio mediante il quale tratta dati personali per conto del delegato del titolare, dopo aver accertato il data breach, ha il compito di segnalare ai ruoli e alle strutture preposte l'accaduto fornendo fattiva collaborazione.

6.2 Descrizione del processo

Il Processo di gestione degli eventi di violazione dei dati Personali consta delle seguenti fasi:

- *Segnalazione*: tutti gli eventi che potrebbero presentare rischi di Data Breach possono essere rilevati sia da soggetti interni (per soggetti interni si intendono anche il Delegato del Titolare, l'RPD e il Settore Agenda Digitale) che da soggetti esterni. Tali eventi devono essere immediatamente segnalati al Settore Agenda Digitale. In questa fase è compresa la seguente attività:
    - *Segnalazione evento anomalo o violazione sicurezza dati personali [1.1].*
- *Archiviazione*: il Settore Agenda Digitale, avendo in carico la tenuta e l'aggiornamento del "Registro regionale degli incidenti sui dati personali", dovrà registrare la segnalazione ricevuta e dovrà tracciare l'attività svolta, sia in caso di accertamento positivo che negativo della violazione. Questa raccolta di informazioni consentirà all'autorità di controllo di verificare il rispetto della normativa. In questa frase sono comprese le seguenti attività:
    - *Registrazione segnalazione [2.1];*
    - *Archiviazione segnalazione con evidenza di analisi, eventuali misure adottate e comunicazioni effettuate [2.2].*
- *Valutazione e misure*: ricevuta la segnalazione, il Settore Agenda Digitale provvede alla comunicazione dell'accaduto al RPD, al delegato del Titolare e al Settore Datore di Lavoro. Procede quindi all'analisi della segnalazione per valutarne la gravità avvalendosi, se necessario, del Settore Datore di Lavoro. Se viene accertata la violazione, determina le misure di contenimento e contrasto per arginare la violazione e attiva le strutture preposte all'attuazione delle misure individuate accertandosi dell'avvenuta attuazione. Queste attività vengono svolte con la collaborazione del Settore Datore di Lavoro, tenendo informato il RPD. In questa fase rientrano le seguenti attività:
    - *Inoltro della segnalazione a Delegato del Titolare, a RPD e Settore Datore di Lavoro [3.1];*
    - *Valutazione gravità evento [3.2];*
    - *Collaborazione per valutazione gravità evento [3.2.1*] (da parte del Settore Datore di Lavoro)*;*
    - *Determinazione misure di contenimento e contrasto [3.3];*
    - *Collaborazione per determinazione misure di contenimento e contrasto [3.3.1]* (da parte del Settore Datore di Lavoro);

- *Attivazione delle strutture preposte all'attuazione delle misure di contenimento e contrasto (Incident response team) [3.4]* (Processo in carico ad altro gruppo);
- *Collaborazione per attivazione delle strutture preposte all'attuazione delle misure di contenimento e contrasto [3.4.1]* (da parte del Settore Datore di Lavoro);

- *Notifica*: se dall'analisi emerge la necessità dell'invio della notifica al Garante e/o dell'invio della comunicazione agli Interessati, le notifiche predisposte con la collaborazione del Settore Datore di Lavoro e del RPD, devono essere inviate dal Delegato del Titolare ai destinatari. Queste le attività previste:
  - *Invio notifica al Garante [4.1];*
  - *Collaborazione per notifica al Garante [4.1.1]* (da parte del RPD)*;*
  - *Collaborazione per notifica al Garante [4.1.2]* (da parte del Settore Datore di Lavoro);
  - *Invio comunicazione all'Interessato [4.2];*
  - *Collaborazione per comunicazione all'Interessato [4.2.1]* (da parte del RPD);
  - *Collaborazione per comunicazione all'Interessato [4.2.1]* (da parte del Settore Datore di Lavoro).

6.3 Diagramma del processo

Nella successiva tabella si riporta la legenda dei simboli utilizzati al fine di rappresentare graficamente il processo di gestione degli eventi anomali e degli incidenti.

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

Tabella 10: Legenda del Processo di gestione degli eventi anomali / incidenti

Nella figura seguente viene mostrato lo schema definito per il processo di gestione degli eventi anomali e degli incidenti.

*: Per soggetti interni si intendono anche il Delegato del Titolare, l'RPD e il Settore Agenda Digitale stesso:

Figura 1: Workflow del Processo di gestione di eventi anomali / incidenti

6.4 Matrice RACI

Qui di seguito viene fornita la matrice RACI che riassume in forma tabellare ruoli e responsabilità dei vari attori coinvolti nel processo di gestione degli eventi anomali e degli incidenti.

	Registrazione segnalazione	*Inoltro segnalazione*	*Valutazione gravità e Determinazione misure*	*Attivazione Incident response team*	*Invio notifica e comunicazione*	*Archiviazione segnalazione*
Soggetto interno / esterno						
Settore Agenda Digitale	A/R	A/R	R	A/R		A/R
RPD		I	I	I	C	
Settore Datore di Lavoro		I	C	C	C	
Delegato del Titolare		I	A		A/R	

R=Responsable: ruolo che esegue materialmente un'attività
A=Accountable: ruolo che ha la responsabilità sul risultato dell'attività
C=Consulted: ruolo che collabora con il *Responsable* per l'esecuzione dell'attività
I=Informed: ruolo che deve essere informato dell'attività

Tabella 11: Matrice RACI

6.5 Gestione di eventi segnalati da responsabili di trattamenti esterni

Se un responsabile di trattamenti esterni di Regione Calabria si accorga o venga a conoscenza di una possibile violazione di dati personali nell'ambito dell'erogazione di un servizio, questi ha l'obbligo di effettuare una prima analisi dell'accaduto. Se accerta che si è in presenza di data breach invia la segnalazione al Delegato del Titolare per il quale eroga il servizio, al Settore Agenda Digitale e al RPD fornendo tutte le informazioni utili per una corretta valutazione e gestione dell'evento. Gli attori così coinvolti procederanno come previsto dal processo descritto nei paragrafi precedenti.

7 SANZIONI PREVISTE

Le procedure relative ai data breach, illustrate nei paragrafi precedenti e previste dagli art. 33-34 del GDPR, rientrano tra gli obblighi del titolare e del responsabile del trattamento. Gli aspetti sanzionatori per la violazione di tali obblighi è normata dall'art. 83 par. 4 del GDPR che prevede sanzioni amministrative pecuniarie fino a 10.000.000 €. In aggiunta, l'art. 82 par. 1 del GDPR prevede che "Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento". Vi è da ricordare che la sanzione applicabile tiene conto di alcuni fattori che possono mitigare o aggravare la violazione. Tali

fattori sono elencati nell'art. 83 par. 2 del GDPR per cui, ad esempio, l'essere intervenuti con tempismo per ridurre la gravità, la natura e la durata della violazione può essere considerato dall'autorità come attenuante nell'erogazione della sanzione.

8 REGISTRO DEGLI INCIDENTI

L'applicativo adottato da Regione Calabria per la gestione degli adempimenti relativi al GDPR fornisce la possibilità di alimentare e manutenere il registro degli incidenti.

Dalla schermata principale, il menu a sinistra permette di accedere alla sezione del registro degli incidenti:

Figura 2: Menu per accesso Registro Incidenti

Questa sezione fornisce all'utente un insieme di campi che consente la memorizzazione di ogni singolo elemento utile a ricostruire la violazione e rendere conto delle azioni intraprese per fronteggiarla. Nelle schermate seguenti l'insieme dei campi compilabili da parte dell'utente in relazione alla singola segnalazione di violazione riscontrata.

Registro Incidenti

Inserisci i seguenti dati

incidente *

data nota

☐ è nota la data in cui è avvenuto il data breach

data scoperta incidente

descrizione

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

dove è avvenuta la violazione

Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

tipo di violazione

Aggiungi

dispositivo oggetto di violazione

Aggiungi

sistemi coinvolti

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

dati violati

Aggiungi

gravità della violazione *

- - -

misure organizzative di sicurezza adottate

- ☐ nomina per iscritto personale
- ☐ istruzioni per il trattamento
- ☐ accesso controllato
- ☐ armadi chiusi
- ☐ procedura modifica credenziali
- ☐ policy aziendali
- ☐ formazione
- ☐ nomina per iscritto responsabili esterni

misure tecniche di sicurezza adottate

- [ ] autenticazione
- [ ] autorizzazione
- [ ] cifratura dei dati
- [ ] separazione
- [ ] firewall
- [ ] antivirus
- [ ] business continuity
- [ ] disaster recovery
- [ ] intrusion detection
- [ ] vulnerability assessment/penetration test

la violazione implica notifica agli interessati

- [ ] Ci sono probabilità di rischi o danni alle libertà e diritti degli interessati

contenuto notifica interessati

interventi effettuati per la risoluzione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

numero interessati *

violazione risolta

- [ ] La violazione è stata risolta

data risoluzione

notifica al Garante

- [ ] La violazione è stata notificata al garante

data notifica al Garante

tag

Figura 3: Campi Registro Incidenti

9 ESEMPI DI VIOLAZIONI DI DATI PERSONALI

Gli esempi che seguono, riportati nel documento WP 250, rev.01 “Linee-guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679” - Gruppo di lavoro Articolo 29 per la protezione dei Dati, forniscono diversi scenari nei quali si stabilisce se è necessaria la notifica all’autorità di controllo e all’interessato.

Esempio	Notifica all’autorità di controllo	Comunicazione all’interessato	Note/Raccomandazioni
Un titolare del trattamento ha memorizzato il backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata nel corso di un’effrazione.	No.	No.	Nella misura in cui i dati sono crittografati con un algoritmo, esistono backup dei dati, la chiave unica non è compromessa e i dati possono essere ripristinati in tempo utile, questa violazione può non essere notificata. Tuttavia, se in un secondo momento vi è compromissione, la notifica diventa necessaria.
Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico a tale servizio, vengono sottratti i dati personali di persone fisiche. Il titolare del trattamento ha clienti in un unico Stato membro.	Sì, segnalare all’autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per le persone è elevata.	
Una breve interruzione di corrente della durata di alcuni minuti nel call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare e accedere alle registrazioni che li riguardano.	No.	No.	Non si tratta di una violazione soggetta a obbligo di notifica, ma di un evento che può essere registrato ai sensi dell'articolo 33, comma 5. Il titolare del trattamento deve tenere registrazioni adeguate.

Esempio	Notifica all'autorità di controllo	Comunicazione all'interessato	Note/Raccomandazioni
Un titolare del trattamento subisce un attacco di tipo ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Da un'indagine emerge chiaramente che l'unica funzionalità del ransomware era quella di crittografare i dati e nessun altro malware era presente nel sistema.	Sì, segnalare all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, segnalare alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre probabili conseguenze.	Se fosse disponibile un backup e i dati potessero essere ripristinati in tempo utile, la comunicazione /notifica all'autorità di controllo o agli interessati non sarebbe necessaria in quanto non vi sarebbe alcuna perdita permanente di disponibilità o di riservatezza. Tuttavia, se l'autorità di controllo viene a conoscenza dell'incidente per altre vie, può prendere in considerazione un'indagine per valutare il rispetto ai requisiti di sicurezza più generali di cui all'articolo 32.
Una persona telefona al call center di una banca per segnalare una violazione dei dati personali. La persona ha ricevuto l'estratto conto mensile di qualcun altro. Il titolare del trattamento avvia una breve indagine (ossia un'indagine che viene completata entro 24 ore) e conclude con ragionevole certezza che si è verificata una violazione dei dati personali e valuta se vi è un difetto sistemico tale da implicare il coinvolgimento di altre persone.	Sì.	Solo le persone colpite ricevono la comunicazione, se vi è un rischio elevato ed è evidente che altri non sono stati colpiti.	Se, dopo ulteriori indagini, si constata che sono coinvolte più persone, occorre informare l'autorità di controllo e il titolare del trattamento adotta le misure supplementari necessarie per informare le altre persone in caso di rischio elevato.
Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Il mercato subisce un cyberattacco e	Sì, segnalare all'autorità di controllo capofila se si tratta di un trattamento transfrontaliero.	Sì, perché potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe intervenire, ad esempio forzando la reimpostazione della password degli account

Esempio	Notifica all'autorità di controllo	Comunicazione all'interessato	Note/Raccomandazioni
l'aggressore pubblica online nomi utente, password e cronologia degli acquisti.			interessati, nonché adottando altre misure per ridurre il rischio. Il titolare del trattamento dovrebbe inoltre prendere in considerazione altri obblighi di notifica, ad esempio ai sensi della direttiva NIS in qualità di fornitore di servizi digitali.
Una società di hosting di siti web che agisce in qualità di responsabile del trattamento identifica un errore nel codice che controlla l'autorizzazione utente. Il difetto fa sì che ogni utente possa accedere ai dettagli dell'account di qualsiasi altro utente.	In qualità di responsabile del trattamento, la società di hosting di siti web deve informare i suoi clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società abbia condotto una propria indagine, i titolari del trattamento interessati dovrebbero sapere con ragionevole certezza se hanno subito una violazione e quindi è probabile che siano considerati come "a conoscenza della violazione" dal momento in cui vengono informati dalla società di hosting (responsabile del trattamento). Il titolare del trattamento deve quindi notificare la violazione all'autorità di	Se è improbabile che vi sia un rischio elevato per le persone fisiche, non è necessario inviare loro una comunicazione.	La società di hosting di siti web (responsabile del trattamento) deve valutare eventuali altri obblighi di notifica (ad esempio nell'ambito della direttiva NIS in qualità di fornitore di servizi digitali). Se non vi sono prove che tale vulnerabilità sia stata sfruttata con nessuno dei rispettivi titolari del trattamento, può non essersi verificata una violazione soggetta a notifica, ma è probabile che la violazione debba essere registrata o che si tratti di un caso di non conformità ai sensi dell'articolo 32.

Esempio	Notifica all'autorità di controllo	Comunicazione all'interessato	Note/Raccomandazioni
	controllo.		
Le cartelle cliniche di un ospedale non sono disponibili per 30 ore a causa di un cyber attacco.	Sì, l'ospedale è obbligato a notificare la violazione perché potrebbe esservi un rischio elevato per il benessere e la privacy del paziente.	Sì, segnalare alle persone colpite.	
I dati personali di un gran numero di studenti vengono inviati per errore alla mailing list sbagliata con più di 1.000 destinatari.	Sì, notificare la violazione all'autorità di controllo.	Sì, comunicare la violazione alle persone a seconda della portata e del tipo di dati personali coinvolti e della gravità delle possibili conseguenze.	
Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di visualizzare l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se sono coinvolte molte persone, se vengono rivelati dati sensibili (ad es. una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad es. la mail contiene le password iniziali).	Sì, comunicare la violazione alle persone a seconda della portata e del tipo di dati personali coinvolti e della gravità delle possibili conseguenze.	La notifica può non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato solo un numero limitato di indirizzi e-mail.

Tabella 12: Esempi di violazioni

Per consentire una migliore lettura e consultazione del processo descritto in questo documento, viene riportata una rappresentazione grafica dal titolo "**Processo di gestione di eventi anomali / incidenti**".