PROCEDURA PER LA GESTIONE DI DATA BREACH

INDICE DELLE REVISIONI

Revisione	Data	Descrizione	Verifica	Approvazione
V1.0	22 maggio 2018	1 Pubblicazione	RiFerroni	MBeretta

Sommario

1. PREMESSA

La presente procedura descrive le attività e le registrazioni che compongono il processo di gestione delle violazioni dei dati personali (c.d.Data Breach), così come regolamentato dagli artt. 33 e 34 GDPR (di seguito anche "GDPR").

I principi e le regole qui indicate si riferiscono all'insieme dei dati personali presenti in azienda, in qualunque modo raccolti e scambiati.

Tali informazioni possono essere presenti in forme diverse, memorizzate nei server e nei data base aziendali, nei computer in dotazione al personale o possono essere conservate come archivi cartacei e scambiate utilizzando linee di comunicazione, fax, ed altro.

Qualora si sospetti o sia in atto una violazione ai dati personali o alla riservatezza delle informazioni è importante che siano presenti procedure idonee per comprendere tempestivamente la gravità dell'incidente ed il rischio associato, e per mettere in atto contromisure per contenere e ridurre al minimo i potenziali danni ed evitare nuovi possibili rischi.

La presente procedura si applica a tutto il personale, dipendenti e collaboratori, professionisti e terze parti, organizzazioni esterne che abbiano accesso ai locali ed alle infrastrutture e che possano utilizzare per qualunque scopo i dati personali del Titolare, Sagam S.p.A., dei suoi clienti, dei suoi responsabili ed eventuali sub-responsabili.

2. FONTI NORMATIVE

Di seguito sono riportate le fonti normative citate:

- Art. 33 GDPR "Notifica di una violazione dei dati personali all'Autorità Garante"
- Art. 34 GDPR"Comunicazione di una violazione dei dati personali all'interessato"
- WP 250 ENG - Guidelines on Personal data breach notification under Regulation 679

3. TERMINI E DEFINIZIONI

Nella tabella seguente sono riportati i termini e le definizioni di cui all'art. 4 GDPR.

Termine	Definizione
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o

Termine	Definizione
	l'interconnessione, la limitazione, la cancellazione o la distruzione.
Limitazione di trattamento	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Stabilimento principale	a) Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) Con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del Regolamento.
Autorità di Controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.
Autorità di Controllo interessata	Un'Autorità di Controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale Autorità di Controllo; b) gli interessati che risiedono nello Stato membro dell'Autorità di Controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale Autorità di Controllo.

Tabella 1 – Termini e definizioni (art. 4 GDPR)

4. DEFINIZIONE DI DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

Il termine data breach,o violazioni di dati,indica qualsiasi violazione di sicurezza dei dati personali e delle informazioni riservate o commerciali che comporti 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 (cfr. art. 4.12 GDPR).

Il data breach consiste in una o più delle seguenti situazioni:

- "Violazione della Riservatezza": divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "Violazione della Disponibilità": perdita accidentale o non autorizzata di accesso o distruzione di dati personali;
- "Violazione dell'Integrità": alterazione non autorizzata o accidentale dei dati personali.

Ciò può originare da una o più delle seguenti situazioni esemplificative:

- smarrimento o furto di attrezzature informatiche, notebook, smartphone chiavette USB contenenti dati personali;
- infedeltà aziendale causata da personale autorizzato o accesso abusivo al sistema informatico di personale non autorizzato con cancellazione o divulgazione dei dati;
- applicazioni web-based;
- email contenenti *malware*.

Per valutare la gravità del data breach, si ha riguardo all'impatto sulla riservatezza, disponibilità o integrità dei dati personali, nonché al tempo ed alle risorse necessarie per risolvere la violazione.

Quest'ultima, infatti, può comportare una serie di conseguenze tali da causare danni, fisici, materiali o immateriali alle persone fisiche.

Tali effetti includono la perdita di controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, decifratura non autorizzata della pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale e qualsiasi altro significativo svantaggio economico o sociale per tali individui.

Il GDPR, all'articolo 33, prescrive che il Titolare del trattamento notifichi 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 sia 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 non sia effettuata entro 72 ore, dovrà essere corredata dei motivi del ritardo.
Sul punto, si veda quanto previsto a pagina 12 del presente documento.

Laddove si ravvisi siffatto rischio di effetti negativi per i diritti e libertà delle persone fisiche, il successivo art. 34 GDPR impone al Titolare del trattamento di comunicare la violazione agli interessati senza giustificato ritardo, utilizzando un linguaggio semplice e chiaro.
A tal riguardo, il Considerando 87 specifica che tali comunicazioni debbano essere effettuate non appena ragionevolmente possibile, in stretta collaborazione con l'Autorità di controllo e nel rispetto

degli orientamenti impartiti da questa o da altre autorità competenti, quali le autorità incaricate dell'applicazione della legge.

Nello specifico si deve, oltre indicare la natura della violazione e dei dati personali:

a) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto presso cui ottenere più informazioni;
b) descrivere le probabili conseguenze della violazione dei dati personali;
c) 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.

Lo stesso articolo 34 specifica, tuttavia, che la comunicazione all'interessato non è sempre obbligatoria qualora ricorra anche solo una delle seguenti condizioni:

- 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;
- 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;
- 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.

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5). Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Poiché un attacco può compromettere i dati personali è di fondamentale importanza avere un'organizzazione, una procedura, e un referente che in caso di attacco possa intervenire il più rapidamente ed efficacemente possibile al fine di mettere in pratica le più appropriate azioni per minimizzare le conseguenze in caso di perdita, furto, distruzione di device e altri servizi causati dall'incidente e per aumentare la protezione del sistema.

5. REFERENTE DEL PROCESSO E TEAM DI SUPPORTO PER GLI INCIDENTI

Il referente del processo di gestione delle violazione dei dati personali è il **Referente Privacy (**espressamente nominato), che può essere coadiuvato da un Team di Supporto per gli incidenti (di seguito anche solo "Team").
L'obiettivo del Team è di garantire un intervento tempestivo non appena si manifesta, o anche solo si sospetti,un data breach, al fine di valutarne l'impatto, per arginare i danni e ripristinare i servizi.

Il Team può essere composto oltre che dal **Referente Privacy** da una persona e/o più persone da lui delegata/e che in sua assenza assumeranno la responsabilità della gestione del Data Breach, oltre che altre funzioni aziendali che ne sono parte permanente, e da altre ancora interne o esterne che sono coinvolte di volta in volta nella gestione dei singoli casi al fine di assicurare le necessarie competenze e responsabilità.

Funzioni del Team di supporto all'Incidente:

- i sistemisti e gli amministratori di sistema che assicurano le necessarie relative competenze;

- il Referente Privacy che verifica il rispetto delle procedure aziendali ed è incaricato delle comunicazioni all'interno e verso gli Enti di Riferimento Normativi.

Altre funzioni aziendali possono essere coinvolte secondo necessità:

- la Funzione o il personale che ha rilevato il Data Breach;
- Human Resources (Responsabile del Personale) quando il data breach ha impatto sui dati del personale dell'azienda;
- i soggetti apicali/Governance.

Eventuali funzioni esterne coinvolte possono essere:

- Enti Governativi e quindi Polizia Postale cui segnalare indirizzi IP responsabili e Garante della Privacy;
- clienti e fornitori coinvolti;
- professionisti incaricati.

Qualora nessun componente del Team si attivasse o comunque desse riscontro nel tempo di 15 minuti, perché il telefono è occupato o per altre esigenze personali o aziendali è necessario attivare con un processo di escalation le altre funzioni aziendali .In tal senso si deve procedere con l'invio di un'e-mail che comunichi il data breach e, a seguire, qualsiasi ulteriore metodo di comunicazione che assicuri una tempestiva risposta.

All'uopo si riportano nel documento allegato le principali informazioni di contatto, indirizzo di posta, numero di telefono, numero identificativo dell'ufficio del personale del Team:

- Referente Privacy, funzione principale;
- Funzione IT;
- Amministratori di Sistema.

6. PROCESSO DI GESTIONE DELLA VIOLAZIONE

Il Titolare ha l'obbligo di identificare l'incidente di sicurezza, valutarne l'impatto sulle informazioni aziendali e sui dati personali. L'art. 33, paragrafo5 del Regolamento EU 2016/679, prescrive l'obbligo di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ne discende che le attività di rilevamento dell'incidente, come le successive fasi di trattamento, devono essere registrate riportando per ciascuna violazione le conseguenze ei rimedi messi in atto; altresì devono essere tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti. È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica all'Autorità di Controllo.

Vengono identificate le seguenti fasi che devono essere gestite in caso di violazione o di sospetta violazione.

Fase 1 – Attività di preparazione

Questa fase è importante per determinare la capacità di risposta al fine di prevenire gli incidenti assicurando che le reti, i software, i sistemi siano sufficientemente protetti, il personale formato, le risorse adeguate per rendere il rischio residuo dell'organizzazione accettabile.

Sono verificate le strategie di contenimento rese disponibili per ciascuno dei principali tipi di incidente, con i relativi piani di azione tenendo conto dei precedenti incidenti, e migliorando le capacità di intervento successive.

La disponibilità e l'utilizzo di soluzioni software strumentali alla protezione, prevenzione e individuazione dalle intrusioni dei sistemi informatici, di Antivirus e Antispam,di altri software specifici di analisi dell'integrità dei dati, dei log di sistema operativo e dei device di rete, possono aiutare a valutare se si è verificato un incidente, e quindi il tipo, la misura e la dimensione. Non meno importantisono le segnalazioni degli amministratori di sistema e del personale dell'azienda che possono rilevare sintomi di incidenti.

Anche in caso di indicatori positivi non è detto che un incidente sia in corso, ma è ragionevole agire come se lo fosse ed attivarsi di conseguenza. Il **Referente Privacy** ha la responsabilità di analizzare tutti i segnali, per valutare la situazione documentando e registrando passo dopo passo, lo status dell'incidente, le informazioni correlate, e qualunque azione venga intrapresa dal momento in cui è rilevato al momento in cui è risolto l'incidente.

Fase 2 - Segnalazione della Violazione e prime azioni di contenimento

Una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, può provocare perdita di riservatezza, furto di dati personali o sociale oltre che compromettere altri sistemi in aggiunta all'eventuale obbligo di notifica entro 72 ore all'Autorità.

Il personale che sospetta o rileva una violazione deve immediatamente mettere in atto contromisure atte a contenere e limitarne l'impatto e se possibile arrestare la violazione, attivare il Referente Privacy, il Referente per la sicurezza delle informazioni o gli amministratori di sistema per eseguire lo shutdown dei sistemi, revocare eventuali privilegi a personale non autorizzato, procedere se ritenuto necessario al backup dei sistemi e ad eventuali altre azioni ritenute necessarie.

Senza ingiustificato ritardo, deve avvertire il personale del Team ed il proprio manager e compilare le informazioni richieste nel "Registro delle Violazioni" e quest'ultime dovranno essere inoltrate a mezzo mail al **Referente Privacy**:

- cognome, nome, sede, ruolo, telefono ed indirizzo di posta di chi ha scoperto la violazione;
- riferimenti del proprio responsabile diretto e dell'unità organizzativa di appartenenza;
- data e ora in cui l'evento è stato scoperto o sospettato;
- natura, modalità e la durata della violazione;
- sistemi e informazioni violate, quantità, tipo e relativo livello di riservatezza;
- fattori di impatto, funzionale, perdita di dati;
- indicare se i dati violati hanno qualche ulteriore livello di protezione, es. criptazione;
- riferimenti di eventuale personale a conoscenza o testimone dell'evento;
- azioni immediatamente intraprese per contenere l'incidente ed evitare il ripetersi;
- possibile causa della violazione:
  - computer, smartphone, memorie e dischi USB rubati persi o lasciati temporaneamente incustoditi, oppure smaltiti in modo inadeguato;
  - furto smarrimento o condivisione della password o di altre informazioni di autenticazione
  - negligenza del personale che utilizza password semplici e facilmente identificabili;

  - negligenza del personale per divulgazione non autorizzata di informazioni protette e riservate o superficialità nel trattare ed trasmettere dati;
  - abuso di privilegi in ambiente di rete che possono determinare modifiche ai dati o installazione di software non autorizzato;
  - furto di documenti cartacei contenenti informazioni personali o riservate lasciati incustoditi sulla scrivania o alla fotocopiatrice oppure smaltiti in modo inadeguato;
  - inadeguate misure di sicurezza e di protezione che lasciano i sistemi vulnerabili e consentono attacchi di hacker o di organizzazioni esterne attuati mediante software che bypassano i sistemi di sicurezza, es firewall, per accedere ai data base aziendali.
- indicazione e descrizione dei possibili rischi per i diritti e le libertà degli interessati;

Il personale che rileva la violazione deve porre particolare attenzione sulla necessità di conservare e non alterare nessuna prova della violazione per rendere possibili ulteriori successive indagini.

Tutte le informazioni relative alla violazione devono essere considerate riservate e comunicate esclusivamente al Referente Privacy o agli altri eventuali membri del Team, che gestirà la violazione valutandone il rischio e le conseguenti azioni da mettere in atto.

Fase 3 - Gestione della Violazione

Il **Referente Privacy** dopo aver espletato le opportune prime azioni di contenimento, deve analizzare:

- le modalità con cui si è verificata la violazione;
- se sono state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione previste per garantire un adeguato livello di sicurezza delle informazioni e dei dati personali;
- la proprietà dei dati violati, e quindi se sono state violate informazioni appartenenti a personale interno o ai clienti diSagam S.p.A.;
- valutare il rischio di utilizzo e le possibili conseguenze della violazione per Sagam S.p.A. e per il proprietario del dato o dell'informazione violata e della conseguente necessaria notifica;
- raccomandazioni e valutazione di azioni migliorative per i futuri interventi al fine di evitare il loro ripetersi.

Il **Referente Privacy** deve valutare la necessità di eseguire ulteriori indagini intervistando il personale coinvolto nella violazione eventualmente aggiornando il "Registro delle Violazioni", e collaborando con il Team, coinvolgendo secondo necessità le altre funzioni presenti coinvolte:

- Human Resources;
- altro personale dell'organizzazione i cui dati sono stati violati;
- Studio o Reparto Legale/ Consulenti Privacy.

La Funzione IT si deve attivare per:

- conservare le informazioni necessarie a mantenere le prove della violazione eseguendo backup dei sistemi, copia dei dischi e delle memorie e dei log presenti per poter eseguire se richiesto ulteriori analisi;

- eseguire se necessario lo shutdown del sistema informatico;
- eliminare eventuali malware presenti identificando gli Host danneggiati per attivare il ripristino;
- in caso di abuso di privilegi in ambiente di rete revocarli immediatamente e verificare quali sistemi dispositivi o cartelle sono state violate e analizzando i relativi log, identificando quali operazioni o attività sono state eseguite nel periodo cui si sospetta essere stata presente la violazione;
- in caso di accesso esterno (logon) non autorizzati, identificare gli indirizzi IP e le applicazioni violate;
- cambiare immediatamente le password violate anche solo potenzialmente, informandone il personale interessato e reimpostando la definizione delle password se ritenute deboli;
- cercare di recuperare le informazioni perse o danneggiate utilizzando se possibile backup di ripristino, ricostruendo file danneggiati con precedenti versioni pulite, e se necessario installando patch, modificando il set di regole del firewall per aumentare la sicurezza, monitorando con attenzione log dei principali sistemi di rete;
- in caso di furto di notebook ed altri dispositivi mobili identificare le informazioni memorizzate e disabilitare gli accessi di eventuali account associati;
- fornire la corretta informazione al personale per aumentare il livello di vigilanza sul sistema.

In caso di violazione attribuibile a personale interno che ha erroneamente ricevuto informazioni, le stesse devono essere restituite, distrutte o cancellate confermandolo per iscritto.

In caso di divulgazione non autorizzata di informazioni riservate attribuibile a terze parti, devono essere valutate le possibili azioni legali; in caso di violazioni attribuibile a personale interno devono essere valutate le possibili azioni disciplinari legate al grado di gravità e pericolosità della violazione.

Fase 4 – Registrazione e Valutazione

Il **Referente Privacy**, nel momento in cui è informato circa una violazione dei dati personali, ha la responsabilità di interfacciarsi con il soggetto che ha effettuato la segnalazione e raccogliere tutte le informazioni necessarie per analizzare l'evento occorso e attivare le opportune funzioni affinché pongano in essere eventuali necessarie misure di mitigazione per la gestione della violazione occorsa o ancora in corso.

Le informazioni da registrare, a cura del **Referente Privacy**, nel Registro delle violazioni dei dati personali, sono riportate nella tabella seguente.

Informazioni	Descrizione
▪Origine segnalazione	▪Dipendente/collaboratore ▪Amministratore di Sistema ▪Responsabile del trattamento
▪Date e ora segnalazione	▪Data e ora in cui la violazione è stata rilevata (tale indicazione è molto importante poiché dal momento in cui vi è consapevolezza di una violazione partono le 72 ore entro cui deve essere effettuata l'eventuale notificazione all'Autorità Garante)
▪Descrizione natura violazione	▪Dispositivi oggetto di violazione ▪Tipologia di violazione ▪Violazione della riservatezza dei dati personali ▪Violazione della disponibilità dei dati personali

	▪Violazione dell'integrità dei dati personali ▪Categorie interessati ▪Numero interessati ▪Categorie di dati personali
▪Indicazione e descrizione dei possibili rischi per i diritti e le libertà degli interessati	▪Indicare gli effetti negativi per gli interessati derivanti dalla violazione: ▪la perdita di controllo sui propri dati personali ▪la limitazione dei loro diritti ▪discriminazione ▪furto d'identità o frode ▪perdita finanziaria ▪danno alla reputazione ▪perdita di riservatezza dei dati personali protetti dal segreto professionale ▪qualsiasi altro significativo svantaggio economico o sociale
▪Valutazione della probabilità di realizzazione dei rischi per i diritti e le libertà degli interessati	▪Indicare la probabilità di realizzazione degli effetti negativi per gli interessati derivanti dalla violazione, anche alla luce delle misure di sicurezza in essere: ▪probabilità BASSA (notificazione all'Autorità Garante) ▪probabilità ALTA (notificazione all'Autorità Garante e comunicazione agli interessati)
▪Misure adottate/di cui si propone l'adozione per contrastare la violazione e/o attenuarne i possibili effetti negativi	▪Descrivere le misure adottate/che si propone di adottare

Tabella 2 – Informazioni da inserire nel Registro delle violazioni dei dati personali

La documentazione delle violazioni dei dati personali è da effettuare per rispondere a quanto stabilito dall'art. 33, paragrafo 5, Regolamento EU 2016/679, ovvero

> *"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"*.

Fase 5– Notifica della Violazione

Violazione dei dati personali

Il **Referente Privacy,** deve notificare il data breach occorso all'Autorità Garante senza ingiustificato ritardo (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 i cui dati sono stati violati. Qualora la notifica all'Autorità Garante non sia effettuata entro 72 ore la stessa deve essere corredata dei motivi del ritardo.

L'eventuale ritardo non giustificato nella notifica pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione previste dall'art.58 GDPR ovvero avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, ordine di sospendere flussi di dati, e sanzioni amministrative il cui importo secondo l'art. 83 GDPR, può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente.

I considerando 75 e 76 del GDPR suggeriscono che occorre tenere in considerazione sia la probabilità che la gravità del rischio per i diritti e le libertà delle persone, in ragione della natura, sensibilità e volume dei dati, numero degli individui coinvolti, facilità di identificazione, gravità e conseguenze degli stessi. Non è richiesta notifica se la violazione non costituisce un probabile rischio per l'individuo. Per esempio, qualora i dati violati sono criptati, la chiave non è compromessa ed è stata generata con soluzioni software non a disposizione di qualsiasi persona non autorizzata ad accedervi, rendendo i dati almeno in linea di principio incomprensibili, se esiste una copia di backup non è necessaria la notifica. È evidente che se la chiave di crittografia è compromessa o il software di crittografia o il suo algoritmo è vulnerabile, esiste un rischio per i diritti e le libertà delle persone fisiche e la notifica può essere richiesta.

La notifica all'Autorità Garante deve contenere le seguenti informazioni:

- descrizione della 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;
- indicazione del nominativo e i dati di contatto dell'eventuale Data Protection Officer o del Referente Privacy o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte diSagam S.p.A.per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

L'Articolo 33, paragrafo 4, Regolamento EU precisa che qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Per esempio in caso di violazioni più complesse, come per alcuni incidenti di sicurezza informatica può essere necessario un'indagine più approfondita per stabilire pienamente la natura della violazione e la misura in cui i dati personali hanno stata compromessa.

Il modello da utilizzare per eventuale notificazione al Garante è **"Modulo Data Breach"** disponibile sul sito www.garanteprivacy.it

Insieme alla notifica all'Autorità Garante, il **Referente Privacy** nel caso di violazione dei dati personali suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, deve comunicare la violazione agli interessati senza ingiustificato ritardo, al fine di consentire agli stessi di prendere le precauzioni necessarie atte a proteggersi mitigando il rischio.

La comunicazione eseguita in stretta collaborazione con le Autorità competenti, deve essere diretta e trasparente (per esempio eseguita via mail o sms) e deve riportare le medesime informazioni sopra indicate per l'Autorità Garante, formulare raccomandazioni necessarie alla persona fisica interessata per attenuare i potenziali effetti negativi della violazione.
In particolare, la comunicazione deve riportare le lettere b) c) e d) del paragrafo 3 del l'art. 33, che per chiarezza e completezza si riportano sotto:

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".

La comunicazione all'interessato non è necessaria se:

- erano state applicate ai dati personali oggetto della violazione misure tecniche e organizzative adeguate di protezione, in particolare misure destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi quali ad esempio la cifratura;
- sono state successivamente adottate le misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati. Ad esempio,può essere stato subito identificato l'individuo che ha avuto accesso ai dati personali e sono stati presi provvedimenti prima che gli stessi fossero utilizzati per finalità non consentite;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede ad una comunicazione pubblica o ad una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

In alcuni casi, per la natura della violazione e della gravità del rischio, è necessario informare le persone colpite senza indugio anche prima di notificare l'Autorità di Vigilanza.
Qualora la violazione abbia impatto sui dati di più di uno stato membro, l'Autorità di Vigilanza competente è l'autorità capofila, ossia l'Autorità di controllo dello stabilimento principale. In caso di dubbi sull'identificazione dell'autorità di Vigilanza capofila, la notifica può essere fatta all'Autorità di Vigilanza locale (da valutare in base alla dislocazione delle sedi).

Violazione di dati personali presso il Responsabile Esterno

Il Responsabile del Trattamento esterno in relazione a quanto previsto dai contratti con Sagam S.p.A., deve procedere a notificare a quest'ultima nella persona del **Delegato Privacy** (o a persona da lui incaricata in caso di assenza di quest'ultimo) l'accaduto in ordine ad una possibile Violazione dei Dati Personali nel rispetto degli accordi in essere.

Fase 6. Review della Violazioni e Azioni che devono essere messe in atto per prevenirle in futuro.

Il **Referente Privacy** deve garantire che la violazione sia stata sufficientemente analizzata e sia stato predisposto e messo in atto un piano di prevenzione che in base alle cause della violazione adotti contromisure atte ad eliminare o ridurre al minimo i rischi di nuove violazioni e quindi:

- valutare in uno specifico meeting post incidente con il personale coinvolto se le attività di risposta sono state adeguate (modalità e tempi), se le procedure sono corrette, se il personale è risultato idoneo, preparato ed ha seguito le indicazioni delle policy, quali precursori o indicatori dovrebbero essere monitorati per rilevare in futuro incidenti simili;
- introdurre se necessario nuove soluzioni tecnologiche o semplicemente aggiornare i software di protezione, antivirus e antimalware, firewall, tool di monitoraggio di attività sospette o anomale e log per tracciare le operazioni eseguite;
- rivedere se necessario l'organizzazione, i processi e le altre policy aziendali;
- almeno, nei casi più gravi, promuovere un training ai dipendenti per migliorare il processo di risposta alla violazione;

- svolgere azioni periodiche di test dei sistemi, di risposte alla violazione dei dati e più in generale di valutazione dei rischi;
- qualora si riscontri una cattiva condotta del personale interno, segnalarlo al suo Responsabile gerarchico diretto ed alla Direzione del Personale per valutare eventuali azioni disciplinari;
- documentare la valutazione soggettiva delle azioni messe in atto, per ciascun incidente o violazione, dal Team e dall'area o ufficio che è stato attaccato e condividerne i contenuti con la governance.

7. AUDIT

I dati annualmente raccolti sono analizzati per tipologia di incidente e possono essere considerati quali indicatori utili per valutare sia le risposte del Team, che gli eventuali danni dovuti a ritardi da rilevamento, i casi di recidiva, la vulnerabilità delle risorse utilizzate.
Gli stessi possono essere oggetto di audit volti ad identificare inefficienze che debbano essere valutate e corrette, per esempio in relazione a:

- documentazione resa disponibile per ciascun incidente;
- risposte agli incidenti, policy, piani e procedure;
- modello e struttura del Team;
- valutazione dei risultati e necessità di nuove misure, tool, risorse, e training.

Lo studio e la valutazione dei risultati dell'incidente possono essere utili anche ai fini della corretta valutazione del riskassesmented alla necessità di ulteriori azioni.

8. INFORMATIVA AL PERSONALE

La violazione dei dati assume maggiore importanza con l'estensione del numero e quantità di dati gestiti, con la sempre maggiore attenzione alle leggi e alle altre disposizioni in materia di privacy, che consistono in norme e regolamenti più stringenti e prevedono *sanzioni,* in caso di inadempienza e con le richieste dei clienti che richiedono audit accurati (al fine di verificare la solidità ed efficacia dei sistemi di protezione e dell'organizzazione a difesa, con *penali* in caso di violazione delle clausole di riservatezza).

Si richiama l'attenzione del personale sulla necessità di prestare la massima attenzione e di organizzare al meglio le attività lavorative evitando comportamenti che possano essere causa di violazione. Le cause di violazione possono essere molteplici. A titolo puramente esemplificativo e non esaustivo:

- computer, smartphones, memorie e dischi USB ed altri dispositivi aziendali lasciati anche temporaneamente incustoditi;
- password di accesso ai sistemi che non rispettano i requisiti minimi di sicurezza o l'utilizzo di password semplici o facilmente riconducibili e più in generale non coerenti con le regole di utilizzo dei sistemi e delle dotazioni aziendali riportate nelle "Norme di Comportamento" presenti sul portale Intranet dell'azienda;

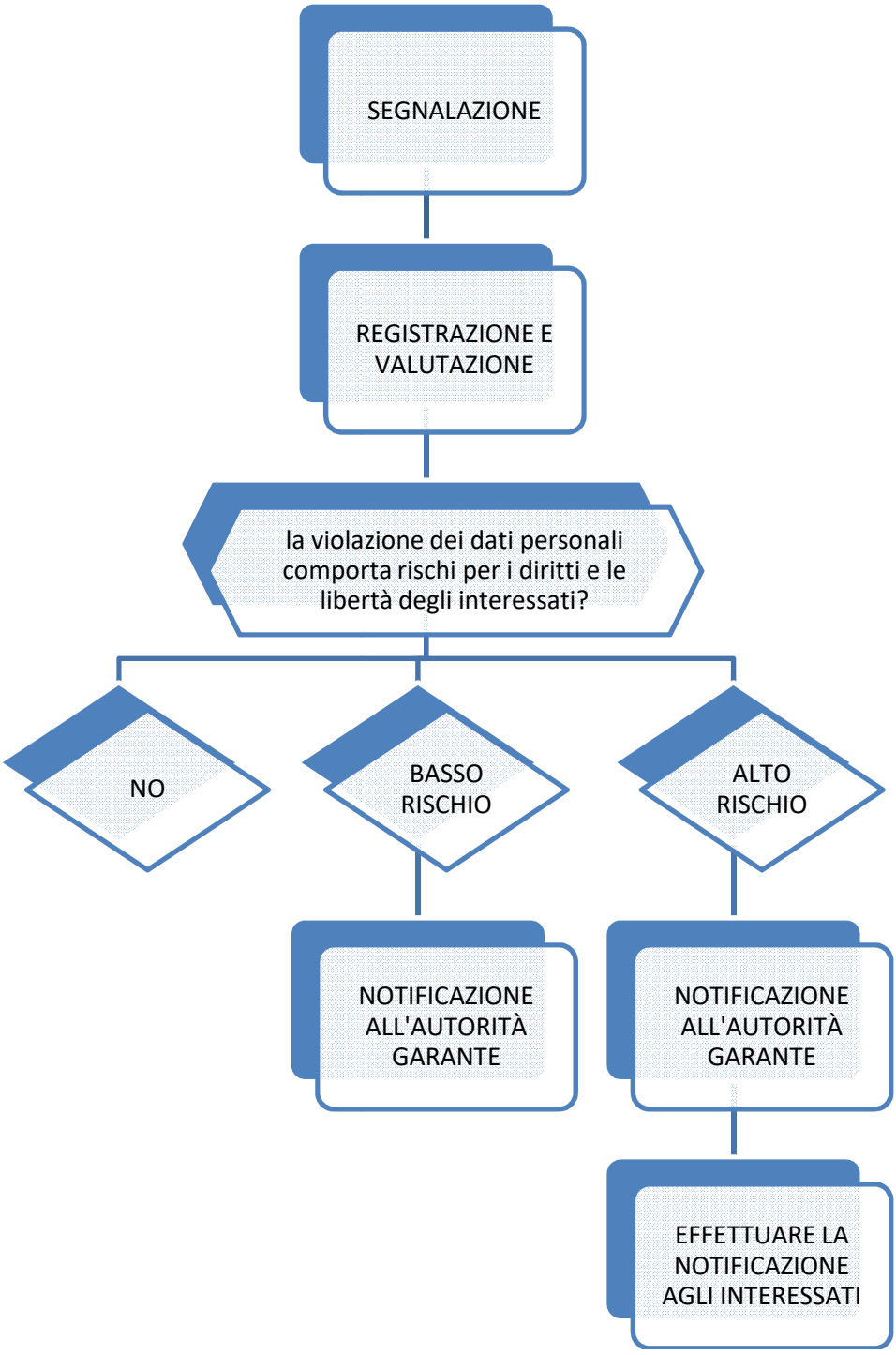
- trasferimento ad altri di dati ed informazioni personali all'interno o all'esterno dell'organizzazione senza il consenso espresso del proprio responsabile gerarchico diretto e/o del personale preposto all'interno dell'organizzazione;
- documenti cartacei contenenti informazioni personali lasciati incustoditi alla fotocopiatrice o sulla scrivania oppure smaltiti in modo inadeguato.

È richiesto a tutti di svolgere un ruolo attivo di prevenzione mettendo in atto anche nei confronti di colleghi condotte e interventi che riducano o elimino i potenziali rischi, segnalando tempestivamente violazioni anche sospette, conservandone le prove e prestando la massima collaborazione con le funzioni preposte al fine di neutralizzarle.

Qualora Sagam S.p.A., anche a seguito di violazioni e perdita di riservatezza dei dati personali ovvero di data breach in genere, che causano danno all'azienda, rilevi comportamenti che possono favorirla o esserne causa non essendo conformi alle indicazioni della presente policy, si riserva la possibilità di agire nei confronti di coloro che possano esserne ritenuti responsabili, riservandosi di poterne addebitare i costi che ne derivano oltre che la possibilità di intraprendere procedimenti disciplinari sanzionati secondo le norme del CCNL.

9. DIAGRAMMA DI FLUSSO DEGLI EVENTI DI DATA BREACH

Il diagramma di flusso seguente riporta la rappresentazione grafica schematica delle attività di segnalazione, registrazione e valutazione, e notificazione e comunicazione delle violazioni dei dati personali.



ALLEGATO ALLA PROCEDURA PER LA GESTIONE DI DATA BREACH

DATI DEI REFERENTI E DEL TEAM DI SUPPORTO

Nome e Cognome	**Mario Ambrogio Beretta**
Ruolo e/o funzione principale	**Consigliere Delegato / Referente Privacy**
Indirizzo di posta elettronica	**databreach@sagam.it**
Numero di telefono	**02 661671**
Dati relativi al Team di Supporto (se presente)	**----------**

Nome e Cognome	**Riccardo Guglielmo Ferroni**
Ruolo e/o funzione principale	**Quality Manager / Referente Privacy**
Indirizzo di posta elettronica	**databreach@sagam.it**
Numero di telefono	**02 661671**
Dati relativi al Team di Supporto (se presente)	**----------**

Nome e Cognome	**Alex Andriotta**
Ruolo e/o funzione principale	**Coordinatore IT / Referente Privacy**
Indirizzo di posta elettronica	**databreach@sagam.it**
Numero di telefono	**02 661671**
Dati relativi al Team di Supporto (se presente)	**----------**

Nome e Cognome	**Marialuisa Cristina Tuzi**
Ruolo e/o funzione principale	**Responsabile MKT / Referente Privacy**
Indirizzo di posta elettronica	**databreach@sagam.it**
Numero di telefono	**02 661671**
Dati relativi al Team di Supporto (se presente)	**----------**