Procedure di Gestione del Trattamento dei Dati personali
Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679

Revisione Difesa Servizi S.p.A. – febbraio 2022

VERSIONI-AGGIORNAMENTI

Versione Originale – Gway srl (approvato Difesa Servizi S.p.A.) – marzo 2021

Revisione Difesa Servizi S.p.A. – febbraio 2022

L'Amministratore Delegato
Avv. Fausto RECCHIA

Sommario

1 RIFERIMENTI NORMATIVI

- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification
- Guidelines on Personal data breach notification under Regulation 2016/679 - WP250 rev.01
- Guidelines on Data Protection Officers ('DPOs' edited by Group of Guarantors Ue WP 29) under Regulation 2016/679 - WP243 rev.01
- 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).

In considerazione del prevalente numero di personale militare impiegato presso Difesa Servizi S.p.A., il presente regolamento è, inoltre, da intendersi "integrativo" delle norme disciplinanti lo *status* di militare di cui al "Testo Unico delle disposizioni in materia di ordinamento militare".
E' da considerarsi, altresì, "integrativo" delle direttive di settore emanate dallo Stato Maggiore della Difesa e da ciascuna Forza Armata di appartenenza attraverso relative Direttive e/o Circolari dello Stato Maggiore Esercito, dello Stato Maggiore Marina Militare, dello Stato Maggiore Aeronautica e del Comando Generale dell'Arma dei Carabinieri.

2 SCOPO E CAMPO DI APPLICAZIONE

Il Presente documento definisce la procedura che **DIFESA SERVIZI S.p.A** adotta per la gestione del Data Breach o violazione di dati personali secondo i requisiti previsti dalla normativa in materia ed in particolare dal Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito anche "**GDPR**").

3 DEFINIZIONI

Il Regolamento UE 2016/679 ("GDPR"), costituisce la normativa principale di riferimento in materia di trattamento dati personali.
Con riferimento alla tutela dei dati personali, sono state, inoltre, emesse linee guida e di indirizzo da parte del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali ("**WP 29**") e del Garante per la Protezione dei Dati Personali (il "**Garante**").
Per una più agevole comprensione si riportano di seguito le definizioni dei termini maggiormente utilizzati:

- "**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 – articolo 4, punto 1), GDPR;
- "**categorie particolari di dati personali**": dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati

genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona – articolo 9 GDPR;

- "**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 – articolo 4, punto 2), GDPR;
- "**registro dei trattamenti**": i titolari e i responsabili del trattamento devono tenere un registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni elencate all'articolo 30 GDPR;
- "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro – articolo 4, punto 3), GDPR;
- "**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 – articolo 4, punto 4), GDPR;
- "**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 – articolo 4, punto 7), GDPR;
- "**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 – articolo 4, punto 8), GDPR;
- "**incaricato**": le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile – [articolo 4, lettera h), Codice Privacy];
- "**principio di accountability**": impone al titolare di mettere in atto le misure tecniche e organizzative adeguate per garantire e per dimostrare che il trattamento è effettuato conformemente alle disposizioni del GDPR tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;
- "**principio di privacy by design**": prescrive al titolare di adottare sia al momento della determinazione dei mezzi del trattamento (cfr. *supra* definizione di trattamento) che all'atto del trattamento stesso, misure tecniche e organizzative adeguate a garantire il rispetto del

GDPR e la tutela dei diritti e delle libertà degli interessati (ad esempio, prevedendo tecniche di data minimization);

- **"principio di privacy by default"**: richiede al titolare di predisporre misure tecniche e organizzative tali da garantire che, per impostazione predefinita, siano trattati esclusivamente i dati personali necessari a ogni specifica finalità del trattamento. Tale principio può essere declinato riducendo la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione e il numero di soggetti che ha accesso ai dati personali;
- **"valutazione di impatto sulla protezione dei dati" o "DPIA"**: valutazione di impatto effettuata dal titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- **"data breach (violazione di dati personali)"**: 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 e tale violazione dei dati personali è suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche.
- **"Registro delle Violazioni"**: E' il documento che contiene le informazioni di rilevamento di tutte le violazioni registrate dal Titolare del Trattamento con le azioni intraprese. E redatto, conservato ed aggiornato a cura del Titolare del Trattamento per mezzo di suoi nominati/delegati.

4 RUOLI E RESPONSABILITA'

Titolare del Trattamento

Notifica la violazione all'Autorità di Controllo competente a norma dell'articolo 55 del GDPR 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 non sia effettuata entro le 72 ore, la stessa deve essere corredata dai motivi del ritardo. Nei casi più gravi la comunicazione della violazione deve essere data anche all'interessato.

Data Protection Officer

Organo interno alla Società che supporta il Titolare del Trattamento nella valutazione della segnalazione ricevuta. Formula indicazioni per il Titolare. Prepara l'eventuale notifica al Garante e l'eventuale comunicazione agli interessati.

Riceve e gestisce le segnalazioni di violazioni su dati personali informando tempestivamente il Titolare del trattamento.

Il DPO gestisce e aggiorna, oltre al Registro delle attività di Trattamento, anche il Registro delle Violazioni.

Comitato Privacy

Organo collegiale interno alla Società che, in ausilio al DPO, supporta il Titolare del Trattamento per l'espletamento delle attività inerenti la valutazione della segnalazione ricevuta.
Supporta il DPO nel formulare indicazioni per il Titolare, nel preparare le eventuali notifiche al Garante e comunicazioni agli interessati.

Personale

Tutto il Personale svolge la funzione di rilevazione delle violazioni qualora vengano interessati direttamente da incidenti su dati personali che trattano in qualità di incaricati.
Rilevata la violazione ne danno pronta comunicazione al DPO senza giustificato ritardo compilando ed inviando la notifica della violazione anche all'indirizzo gdpr@difesaservizi.it .

Responsabili esterni del Trattamento

Svolgono la funzione di rilevazione delle violazioni qualora esse accadano su dati personali trattati per conto del Titolare del Trattamento. Rilevata la violazione ne danno pronta comunicazione al DPO senza giustificato ritardo compilando ed inviando la notifica della violazione anche all'indirizzo gdpr@difesaservizi.it.

5 Violazione dei Dati Personali (Data Breach)

5.1 LA PROTEZIONE DEI DATI PERSONALI

Il Titolare del trattamento di dati deve notificare all'Autorità di Controllo le violazioni di dati personali di cui viene a conoscenza entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della avvenuta violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34 del GDPR.

I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del GDPR.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

Il titolare del Trattamento dovrà in ogni caso documentare sull'apposito registro 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.

5.1.1 TIPOLOGIE DI VIOLAZIONI

Una violazione di dati personali è definita come: "*la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, ai dati personali trattati*".

Le violazioni possono essere classificate in:

- "**violazione della riservatezza**", in caso di divulgazione o accesso (accidentale o non autorizzato) ai dati personali;
- "**perdita della disponibilità**", in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata);
- "**violazione dell'integrità**", in caso di alterazione (non autorizzata o accidentale) dei dati personali.

Possono esservi violazioni che sono combinazioni delle violazioni indicate.

E' bene sottolineare che, mentre tutte le violazioni di dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono violazioni di dati personali.

5.1.2 ACCOUNTABILITY E CONSAPEVOLEZZA DEL TITOLARE

Il Titolare del Trattamento adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio – e pertanto idonee a prevenire ogni violazione di dati personali - implementando direttamente sistemi di protezione dei dati personali o ricorrendo a fornitori esterni indicando loro le misure di protezione e di sicurezza da implementare.

Il Titolare del Trattamento ricorre eventualmente a Responsabili (esterni) del Trattamento per garantire che le misure valutate adeguate a seguito dell'attività di Risk Management effettuata sui singoli trattamenti siano implementate ed efficaci.

Il Titolare diviene "consapevole" della violazione quando ha un ragionevole grado di certezza che un incidente di sicurezza ha causato la compromissione dei dati personali. In alcuni casi può essere relativamente chiaro dallo scenario che si è verificata una violazione mentre in altri ci vorrà tempo per stabilire se i dati personali sono stati violati.
Si deve quindi effettuare una analisi dell'incidente, che rappresenta una fase fondamentale per stabilire se si è in presenza di una violazione e quindi determinare sulla base dei risultati le azioni da compiere entro i tempi fissati e comunque tempestivamente.

Il Titolare del Trattamento, con il supporto del DPO/Comitato Privacy (di seguito "Referenti Privacy"), documenta le violazioni attraverso la redazione, conservazione ed aggiornamento del **Registro delle Violazioni** al sussistere di ogni violazione, indipendentemente dal rischio presentato per i diritti e le libertà degli interessati.

In tale Registro sono indicati tutti gli elementi richiesti dalla normativa vigente, tra cui:

- le circostanze relative alla violazione;
- le sue conseguenze;
- le misure adottate per contrastarla e limitarne gli effetti;
- i dati personali coinvolti; informazioni adeguate per permettere al Titolare di determinare le motivazioni per non aver effettuato la notifica, o averla effettuata in ritardo.

Il Titolare creerà dei fascicoli per ciascuna violazione documentando tutto quanto accaduto[1].

Di seguito è schematizzata l'interazione tra gli attori coinvolti nel processo di gestione delle violazioni di dati personali.

5.2 LA RILEVAZIONE DELLA VIOLAZIONE

I soggetti che possono rilevare un incidente/violazione riguardante dati personali ed essere quindi una possibile Sorgente di rilevazione di violazione dei dati (di seguito "**Sorgente**") sono:

- I Soggetti interni alla società i cui aspetti in materia di violazione sono disciplinati da lettere di autorizzazione al trattamento;
- I Responsabili outsourcers del Trattamento i cui aspetti in materia sono disciplinati da apposito contratto di responsabilità.

Generalmente le violazioni avvengono su sistemi informatici e file digitali, ma si devono considerare come violazioni anche gli incidenti sui documenti cartacei (es nel caso di furto di documentazione o violazione della riservatezza).

Limitatamente ai temi di disponibilità ed integrità è possibile limitare i casi di applicabilità della violazione ai soli eventi che comportino una compromissione irreversibile di tali caratteristiche del dato personale. Negli altri casi la classificazione dell'evento sarà limitata ad un incidente di sicurezza ICT.

Le misure tecniche e organizzative adottate, sia il personale autorizzato, sia i Responsabili del Trattamento devono comunque essere tali da:

- monitorare periodicamente e proattivamente le risorse e gli asset con i dati da proteggere;

[1] Il Garante raccomanda ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante stesso in caso di accertamenti

- rilevare l'avvenuta violazione (appena essa accade o entro un tempo ragionevolmente breve);
- darne comunicazione in tempo ragionevolmente breve al DPO;
- contrastare tempestivamente la violazione al fine di neutralizzarla;
- ripristinare la situazione di normalità pre-violazione.

Rilevato l'incidente/violazione o nel dubbio che si sia verificata una violazione dei dati personali, la Sorgente effettua immediatamente e senza giustificato ritardo la comunicazione ai Referenti Privacy (anche all'indirizzo gdpr@difesaservizi.it), compilando quanto più possibile la scheda di cui all'Allegato A.
E' buona norma inserire nella comunicazione della violazione in copia anche gli eventuali Referenti Interni interessati.

Contestualmente alla rilevazione della violazione, la Sorgente mette in atto tutte le misure necessarie e possibili (anche temporanee) per far cessare quanto prima la violazione e possibilmente i suoi effetti, il tutto a stretto contatto con il Titolare.

5.3 LA GESTIONE DELLA VIOLAZIONE

I Referenti Privacy, ricevuta la comunicazione di incidente/violazione dei dati personali dalla Sorgente, appurano attraverso ulteriori approfondimenti con la Sorgente, i termini e le caratteristiche indicate nella comunicazione (Allegato A), verificando attraverso un check preliminare se si tratti a tutti gli effetti di una violazione.

Ricorrendo gli estremi per una violazione di dati personali, il DPO supportato dal Comitato Privacy, segue i seguenti passi:

1. apre formalmente la procedura di violazione compilando una nuova riga del Registro delle Violazioni;
2. effettua l'analisi della violazione, che viene condotta attraverso la valutazione:
    - delle categorie dei dati violati;
    - delle misure di sicurezza presenti e la loro elusione;
    - delle misure di sicurezza temporanee subito implementabili per bloccare la violazione nel caso essa sia ancora in azione;
    - di eventuali soggetti esterni da allertare collegati ed in relazione con la violazione;
    - delle possibili conseguenze della violazione sui diritti degli interessati;
    - della stima del numero di interessati coinvolti;
    - della necessità di notificare il Garante;
    - della necessità di comunicare agli interessati (cfr. precedente paragrafo 5.5).

3. esprime, sulla base dell'analisi svolta, una valutazione e la condivide con il Titolare del Trattamento al fine di decidere se notificare la violazione all'Autorità Garante e se notificare o meno gli interessati coinvolti;
4. supporta il Titolare nell'effettuazione della notifica al Garante se da effettuare e nella comunicazione agli interessati se ritenuta necessaria;
5. aggiorna in ogni caso il Registro delle violazioni indipendentemente dalla Notifica al Garante, indicando sempre le motivazioni di una mancata notifica o di un ritardo della stessa;
6. chiude, verificato lo stato di conclusione dell'azione di violazione, la procedura e comunica tale chiusura a tutti gli attori coinvolti (titolare, referenti interni, sorgenti), archiviando la documentazione relativa;
7. valuta l'eventuale calendarizzazione di incontri di follow-up della violazione avvenuta con gli attori coinvolti al fine di determinare lo stato delle misure di sicurezza e l'implementazione di nuove misure possibili per evitare la ripetizione della violazione avvenuta.

5.4 LA NOTIFICA ALL'AUTORITA'

Nel caso in cui il Titolare del Trattamento, in base all'analisi svolta dai Referenti Privacy, decida di procedere con la notifica della violazione (Data Breach) all'Autorità Garante, la stessa deve almeno contenere:

- la **descrizione della** natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione;
- il **nome e i dati di contatto del Titolare del Trattamento** o di altro punto di contatto presso cui ottenere più informazioni;
- le **probabili conseguenze della violazione** dei dati personali;
- 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.

Laddove, inizialmente, non siano noti tutti i dati da notificare e risulti impossibile determinare l'estensione della violazione ma piuttosto sono necessari tempi ulteriori per approfondimenti è prevista una "notifica a fasi" verso il Garante. Essa prevede una notifica iniziale indicando le ragioni per una comunicazione parziale.
L'Autorità dovrebbe concordare come e quando le informazioni supplementari dovranno essere fornite. Questo non impedisce al Titolare di fornire ulteriori informazioni in qualsiasi altra fase qualora diventi consapevole di ulteriori dettagli rilevanti da fornire al Garante.

Notificare all'autorità di vigilanza entro le prime 72 ore può consentire al Titolare di assicurarsi che le decisioni relative alla notifica degli interessati siano corrette.

5.5 LA NOTIFICA AGLI INTERESSATI

La comunicazione della violazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno:

a) comunicazione del nome e i dati del Punto di Contatto presso cui ottenere più informazioni (mail privacy gdpr@difesaservizi.it);
b) descrizione delle probabili conseguenze della violazione dei dati personali;
c) descrizione delle 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.

5.6 VALUTAZIONE DEI RISCHI PER I DIRITTI AGLI INTERESSATI

Il Titolare del Trattamento, sulla base di quanto stabilito dal GDPR (considerando 76), con il supporto dei Referenti Privacy, valuta la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio deve essere, infatti, considerato in base a una valutazione oggettiva mediante la quale si stabilisce se i trattamenti di dati comportano un rischio elevato.

Per stabilire la necessità di notifica agli interessati, in caso di violazione dei dati, il considerando 75 del GDPR descrive i fattori utili per valutare i rischi per i diritti delle persone fisiche:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

6 ALLEGATI

6.1 ALLEGATO A

Modello di Segnalazione Data Breach

Segnalazione data breach *Ultimo aggiornamento:*		
0. Responsabile del Trattamento		
Denominazione sociale*:		
Referente da contattare*:	Nome e cognome: Ruolo: Telefono: e-mail:	
1. Dettagli del data breach		
Breve descrizione del data breach*:		
Data / Ora di accadimento:		
Data / Ora di rilevazione*:		
Data / Ora di classificazione*:		
Modalità di rilevazione*:		
Data / Ora di chiusura:	Specificare:	☐ In corso
Nazione in cui è avvenuto il data breach:		
2. Tipologia, perimetro e portata		
Tipologia di Dati Personali oggetto del data breach*:	☐ Dati di profilazione	☐ Dati finanziari
	☐ Dati di localizzazione	☐ Categorie particolari di Dati

	☐ Dati identificativi	☐ Se Altro, specificare:
Volume dei Dati Personali:		☐ Non definito
Tipologia di interessati*:	☐ Clienti	☐ Dipendenti
	☐ Prospect	☐ Collaboratori esterni
	☐ Categorie soggetti vulnerabili	☐ Se Altro, specificare: (es. Fornitori)
Numero approssimativo di interessati:		☐ Non definito
Tipologia di evento*:	☐ Accesso non autorizzato	☐ Distruzione
	☐ Rilevazione	☐ Modifica
	☐ Perdita	☐ Se Altro, specificare:
Causa della violazione:	☐ Illegale	Specificare se causa interna o esterna:
	☐ Accidentale	Specificare se malfunzionamento di sistema o errore umano:
	☐ Altro:	Specificare:
In caso di violazione illegale, quale minaccia ha causato la violazione:	☐ Malware	☐ Insider/Third Party Provider Threat
	☐ Social Engineering	☐ Unauthorised access
	☐ Se Altro, specificare:	
Società del Gruppo impattata*:		
Terze Parti coinvolte*:		

Sistemi IT impattati*:	
3. Danno e mitigazione	
Misure di sicurezza tecniche e organizzative in essere al momento dell'incidente sui sistemi oggetto della violazione:	
Contromisure adottate per indirizzare il data breach e mitigare ulteriori rischi (azioni di mitigazione):	
Contromisure pianificate per rimuovere le vulnerabilità che hanno causato il data breach (azioni di rimedio):	
Data pianificata per l'implementazione azioni di rimedio:	
Funzione responsabile:	
4. Allegati	
Allegare eventuale documentazione a supporto	

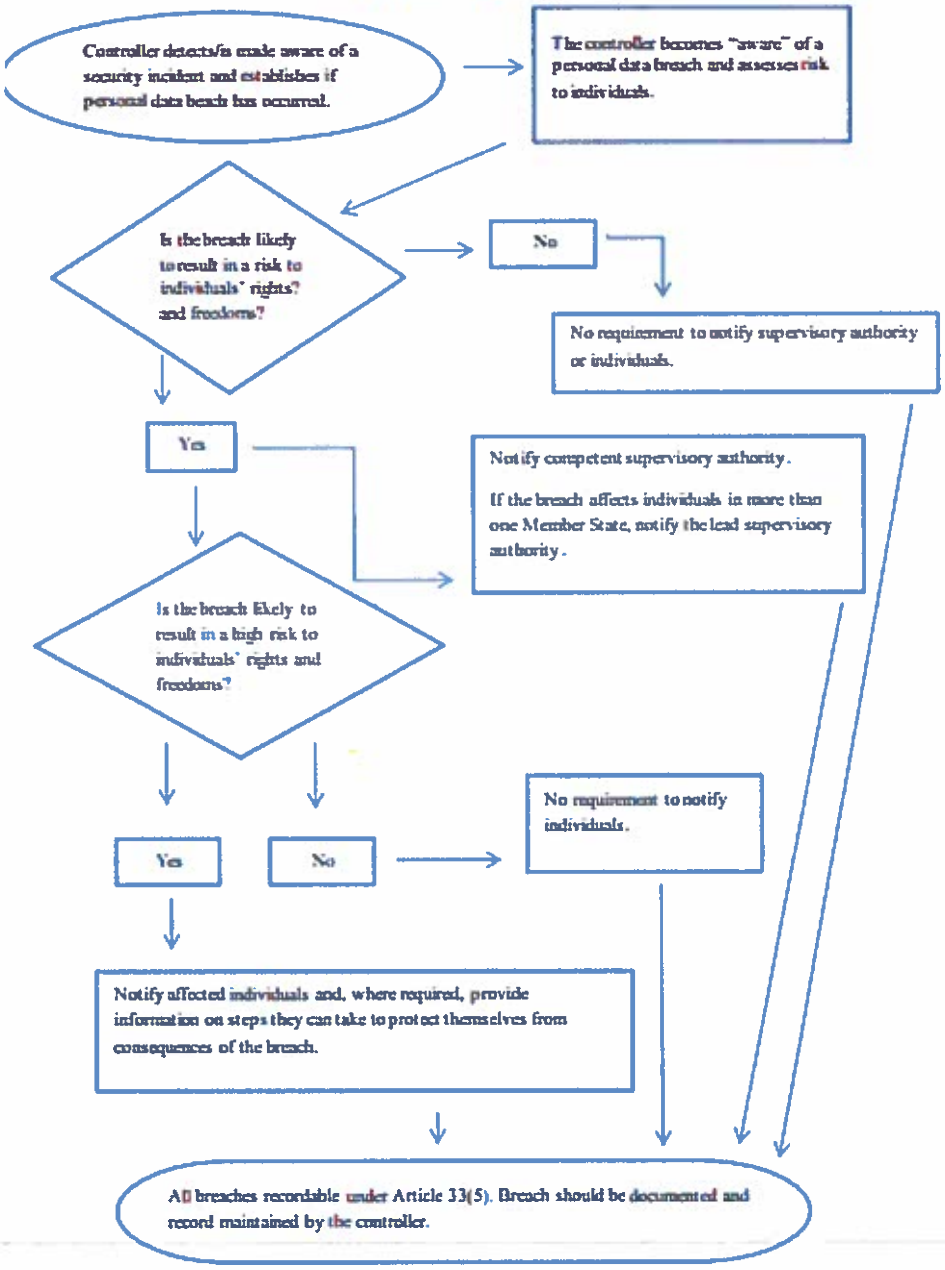
(*) Informazioni da compilare nella prima segnalazione relativa al Data Breach

6.2 ALLEGATO B

Di seguito viene descritto Il workflow realizzato dal WP29 per schematizzare il flusso di gestione di un data breach.

VII. Annex

A. Flowchart showing notification requirements



DIFESA SERVIZI

REGISTRO DELLE VIOLAZIONI (DATA BREACH)

(ai sensi degli art. 33 GDPR nr. 679/2016/UE)

DETTAGLI DELLA VIOLAZIONE							CONSEGUENZE	REAZIONI		
NR. ORDINE	DATA	LUOGO	CAUSE DELLA VIOLAZIONE	ELENCO BANCHE DATI VIOLATE	TIPOLOGIA DI DATI PERSONALI VIOLATI		EFFETTI E CONSEGUENZE DELLA VIOLAZIONE	PIANO DI INTERVENTO	NOTIFICA	MOTIVAZIONE
					DATI COMUNI	DATI PERSONALI PARTICOLARI (DATI SENSIBILI)				
(codice univoco)	(data in cui è avvenuta conoscenza del data breach)	(luogo dove è avvenuto il data breach)	(quali sono state le cause del data breach es. attacco informatico, dipendente infedele ecc)	(individuazione tipologia, posizione e numero delle banche dati violate)	( ) dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro) Dettagli: _____ ( ) situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. ( ) dati inerenti lo stile di vita ( ) situazione economica ( ) situazione finanziaria ( ) situazione patrimoniale ( ) situazione fiscale ( ) dati di connessione: indirizzo IP, login, altro. ( ) dati di localizzazione: ubicazione, GPS, GSM, altro.	( ) Dati inerenti l'origine razziale o etnica ( ) opinioni politiche ( ) convinzioni religiose o filosofiche ( ) appartenenza sindacale ( ) salute, vita o orientamento sessuale ( ) dati genetici e biometrici ( ) dati relativi a condanne penali Dettagli: _____	(descrivere quali sono stati gli effetti e le conseguenze del data breach in termini di danni fisici, materiali o immateriali alle persone fisiche) es. perdita del controllo dei dati, limitazione dei diritti, discriminazione, furto, usurpazione d'identità, perdite finanziarie, pregiudizio della reputazione, perdita della riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica	(indicare quali sono le misure messe in atto dal Titolare del trattamento per contrastare la violazione e prevenire le future violazioni in termini di prevenzione, capacità di rilevare le violazioni, la reazione di contrasto dell'attacco e di mitigazione degli effetti).	( ) al garante ma NON agli interessati ( ) al garante e agli interessati ( ) ritardo nella procedura di notifica	(indicare perché si è provveduto a notificare, non notificare o ritardare la procedura di notifica)