Università degli Studi “G. d’Annunzio”

Procedura
per la gestione delle
violazioni di dati personali

Sommario

1 Introduzione 3
2 Scopo 3
3 Campo di applicazione 3
4 Definizioni 4
5 Normativa di riferimento 6
5.1 Art. 33 - Reg. (UE) 679/2016 - Notifica di una violazione di dati personali all'Autorità di controllo 6
5.2 Art. 34 - Reg. (UE) 679/2016 - Comunicazione di una violazione di dati personali all'interessato ..6
6 Team di risposta alle violazioni ed elementi di valutazione 8
6.1 Team di risposta alle violazioni (*Data Breach Response Team* - DBRT) 8
6.2 Informazioni preliminari per la valutazione delle violazioni 9
7 Descrizione del processo 10
7.1 Rilevazione della violazione di dati personali 10
7.2 Gestione della violazione (valutazione e decisione) 11
7.3 Documentazione della violazione 14
7.4 Analisi post-violazione 14
8 Data breach presso l'Ateneo quando opera in qualità di responsabile (esterno) del trattamento 17
8.1 Obblighi di comunicazione dell'Università quando opera in qualità di responsabile 17
9 Allegati 18
9.1 Allegato 1 - Modulo di documentazione interna della violazione dei dati personali 18
9.2 Allegato 2 – Informativa trattamento dei dati personali relativa alla segnalazione di Data Breach 18
9.3 Allegato 3 - Modello di valutazione della segnalazione 18
9.4 Allegato 4 – Recapiti e nominativi dei componenti del Data Breach Response Team - DBRT 18

1 Introduzione

La normativa vigente in materia di protezione dei dati personali -costituita in via principale dal "Regolamento (UE) 679/2016 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)" (di seguito "Regolamento") e dal "Codice in materia di protezione dei dati personali" (di seguito"Codice") di cui al D.lgs. 196/2003, come modificato dal D.lgs. 101/2018- ha l'obiettivo di garantire la sicurezza e riservatezza dei dati personali oggetto di trattamento, evitando che l'uso non corretto dei dati possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati. Considerato il contesto operativo dell'Università "G. d'Annunzio", la tematica della protezione dei dati personali assume una significativa rilevanza.

I dati personali trattati dall'Università "G. d'Annunzio", in qualità di titolare del trattamento, sono costituiti principalmente da dati personali anagrafici e di contatto e, quando necessario al perseguimento delle finalità istituzionali dell'Università, anche da informazioni riconducibili alla categoria delle "particolari categorie di dati personali" di cui all'art. 9 del Regolamento.

L'Università "G. d'Annunzio" ha predisposto il presente documento nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati.

2 Scopo

Il presente documento descrive le modalità operative adottate dall'Università "G. d'Annunzio" per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento. In particolare viene definito un flusso di attività da porre in essere nel caso in cui dovesse manifestarsi un evento di violazione dei dati personali.

L'obiettivo del presente documento è pertanto di fornire una descrizione generale del processo di gestione delle violazioni di dati personali e delle relative indicazioni operative per poter procedere con la rilevazione, la valutazione ed il contenimento della violazione. E' altresì oggetto di valutazione la necessità di dover procedere con la comunicazione al Garante per la protezione dei dati personali ed eventualmente all'interessato.

3 Campo di applicazione

Per violazione di dati personali (c.d. "data breach"), ai sensi dell'art. 4, n. 12 del Regolamento, si intende "*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"*.

Una violazione di dati personali può di fatto verificarsi a seguito di uno o più degli eventi di seguito indicati. (Si tratta di una elencazione a titolo meramente esemplificativo e non esaustivo)

- Accesso non autorizzato ai dati personali
- Azioni, accidentali o meno, da parte dei soggetti autorizzati al trattamento
- Invio dei dati a un destinatario errato
- Perdita o furto di dispositivi di memoria o computer portatili che contengono dati personali
- Alterazione non autorizzata di dati personali
- Perdita della disponibilità di dati personali

4 Definizioni

Le seguenti definizioni, sancite dall'art. 4 del Regolamento, sono di utilità per poter meglio descrivere lo scenario di riferimento della procedura oggetto del presente documento: questionario in base all'art. 4 del Regolamento:

«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 l'interconnessione, la limitazione, la cancellazione o la distruzione;

«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 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;

«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;

«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;

«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 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;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«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;

«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.

A queste definizioni si affiancano le seguenti, intendendo per:

«banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«**evento sulla sicurezza delle informazioni**»: occorrenza identificata di uno stato di un sistema, servizio o rete, che indichi una possibile violazione di una *policy* sulla sicurezza delle informazioni (*Information Security Policy*) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza;

«**incidente sulla sicurezza delle informazioni**»: evento o serie di eventi sulla sicurezza delle informazioni, indesiderati o imprevisti, che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.

5 Normativa di riferimento

Il processo illustrato nel presente documento descrive le attività da porre in essere nel caso in cui si verifichi una violazione di dati personali che, secondo quanto previsto dagli artt. 33 e 34 del Regolamento, comporta i seguenti obblighi:

- obbligo di notifica al Garante "senza ingiustificato ritardo" e, ove possibile, entro 72 ore (art. 33 del Regolamento);
- obbligo di comunicazione agli interessati, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34 del Regolamento).

5.1 Art. 33 - Reg. (UE) 679/2016 - Notifica di una violazione di dati personali all'Autorità di controllo

1. In caso di violazione di dati personali, il titolare del trattamento notifica la violazione all'Autorità di controllo (nel caso di specie, Garante per la protezione dei dati personali) 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 di dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nella violazione, 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 di 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 di 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 della normativa vigente.

5.2 Art. 34 - Reg. (UE) 679/2016 - Comunicazione di una violazione di 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.

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

3. Non è richiesta la comunicazione all'interessato 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;

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 di dati personali, l'Autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione di dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al par. 3 è soddisfatta.

6 Team di risposta alle violazioni ed elementi di valutazione

6.1 Team di risposta alle violazioni (*Data Breach Response Team* - DBRT)

Il team di risposta alle violazioni è una struttura multidisciplinare cui è demandato l'accertamento della violazione di dati personali l'adozione e la conseguente valutazione delle misure da adottare.

La composizione del team (**Allegato 4 – Componenti del Data Breach Response Team – DBRT**) è costituita dai referenti delle strutture organizzative direttamente coinvolte nella gestione della protezione dei dati personali. La struttura può, alla luce delle specifiche esigenze che possono prospettarsi caso per caso, avvalersi di specifici ulteriori soggetti interni ed esterni alla struttura organizzativa dell'Università, a ciò espressamente incaricati. Il team si impegna a consultare tempestivamente il Responsabile della protezione dei dati personali sulle singole possibili violazioni.

Team di risposta alle violazioni		
Funzione	**Competenza**	**Partecipazione**
Rettore	Rappresentanza legale dell'Università	Componente di base
Direttore Generale	Gestione della struttura organizzativa quale considerata nel suo complesso	Componente di base
Responsabile della Commissione esperti per le attività di supporto per gli adempimenti del GDPR	Conoscenza della normativa vigente in materia di protezione dei dati personali	Componente di base
Responsabile Settore Sistemi informativi e Innovazione tecnologica	Conoscenza dell'infrastruttura di rete, delle misure di sicurezza idonee adottate e delle infrastrutture tecnico-applicative impiegate per il trattamento dei dati	Componente di base
Direttore/Responsabile della struttura organizzativa coinvolta nella violazione	Gestione della struttura organizzativa coinvolta nella violazione	Componente di base, ancorché variabile in base all'area organizzativa in cui si verifica l'evento
Affari Legali	Conoscenza della normativa vigente in materia di protezione dei dati personali e di eventuali ulteriori aspetti legali da valutare	Componente di base

Il team, sentito il parere del Responsabile della protezione dei dati personali, deve assicurare un'adeguata tempestività nella mitigazione delle violazioni, oltre a fornire tutte le risorse necessarie per il contrasto dell'evento e la formulazione di un'adeguata risposta. In caso di eventuale dissenso da parte dell'RPD circa le singole valutazioni effettuate dal DBRT, questo, con le relative motivazioni, andrà documentato annotandolo nel Registro dei Data Breach, gestito dall'ufficio Privacy su mandato del Titolare.

Come già anticipato, se necessario, il team può essere coadiuvato da consulenti esterni, come ad esempio società che si occupano di sicurezza informatica, società di analisi forense dei dati, ecc.

Il Team deve essere preparato alla risposta a presunte o accertate violazioni 24 ore su 24, 7 giorni su 7. A tale scopo, è necessario avere a disposizione la lista aggiornata dei contatti di ogni membro del team. A riguardo l'Ufficio Privacy cura l'aggiornamento dell'elenco dei componenti e dei relativi recapiti (**Allegato 4 – Recapiti e nominativi dei componenti del Data Breach Response Team - DBRT**)

Ancorché non componente di base del team, essendo necessario garantire, sulla base di quanto previsto dall'art. 38, par. 1 del Regolamento, il confronto con il Responsabile della protezione dei dati, il quale deve garantire una pronta collaborazione, si include il medesimo nel sopra citato allegato.

6.1.1 Compiti del Team

Pervenuta una segnalazione di possibile violazione dei dati personali da parte del Titolare, il team dovrà:

a) validare/rispondere alla violazione;
b) predisporre un'appropriata e imparziale investigazione, documentandola correttamente;
c) identificare gli eventuali *asset* da bonificare e tenere traccia delle misure da porre in essere per risolvere le vulnerabilità;
d) coordinarsi con le Autorità se necessario;
e) coordinarsi per la comunicazione verso l'interno e verso l'esterno;
f) rispettare gli obblighi di notifica e di comunicazione;
g) analizzare ogni incidente e tenere traccia della violazione nel registro
h) coinvolgere tempestivamente l'RPD nelle varie fasi al fine di consentirgli di fornire la consulenza al Team e al Titolare documentando eventuali dissensi.

6.2 Informazioni preliminari per la valutazione delle violazioni

Nell'ambito delle valutazioni relative alla gravità (*severity*) delle violazioni dovranno essere tenuti in considerazione i seguenti fattori di rischio per i diritti e le libertà dei soggetti interessati:

a) tipologia di violazione: la tipologia di violazione si configura come parametro per la valutazione del rischio (ad esempio: la violazione dei dati curricolari di tutti gli studenti di un Corso di Laurea è diversa dalla perdita dei dati curricolari di un singolo studente);
b) natura, numero e grado di sensibilità dei dati personali violati;
c) facilità di associazione dei dati violati all'interessato;
d) gravità delle conseguenze per gli interessati e, conseguentemente, valutazione relativa al rischio che i dati personali violati rappresentino un rischio immediato per gli interessati tale da porre in essere frodi o sostituzioni di persona;
e) analisi del contesto nel quale si è verificata la presunta perdita di dati personali;
f) numero di interessati esposti al rischio;
g) caratteristiche del titolare del trattamento.

In particolare all'interno della nozione di "tipologia di violazione" possono ricondursi:

a) (una) violazione sulla riservatezza (c.d. "c*onfidentiality breach"*) quando si verifica un accesso accidentale o non autorizzato ai dati personali o la divulgazione degli stessi;
b) (una) violazione sulla disponibilità (c.d. *"availability breach"*) quando si verifica una perdita o distruzione accidentale o non autorizzata del dato personale;
c) (una) violazione sull'integrità (c.d. "*integrity breach"*) quando si verifica una modifica accidentale o non autorizzata del dato personale.

7 Descrizione del processo

Il processo qui di seguito illustrato descrive le attività da compiere nel caso in cui si verifichi una violazione di dati personali in conformità con quanto stabilito dagli artt. 33 e 34 del Regolamento.

Il processo si articola nelle seguenti fasi:

a) rilevazione di una violazione di dati personali
b) gestione della violazione (valutazione e decisione)
c) risposta all'evento
d) eventuale notifica al Garante per la protezione dei dati personali
e) eventuale comunicazione agli interessati
f) documentazione della violazione

7.1 Rilevazione della violazione di dati personali

La segnalazione di eventi che possono costituire una violazione di dati personali può avvenire per canali interni ed esterni:

A) **Canali interni**

Le segnalazioni di eventi anomalie possono provenire internamente da:

- personale dell'Università: nel caso in cui un autorizzato al trattamento dei dati di secondo livello si accorga di una concreta, potenziale o meramente sospetta violazione di dati personali, questi deve **immediatamente** informare il proprio referente (incaricato di primo livello) della possibile violazione. Quest'ultimo, sulla base di un'analisi preliminare dell'accaduto ravvisati gli estremi per la classificazione quale data breach, dovrà dare immediata comunicazione al Titolare, mediante la compilazione dell'Allegato 1 - Modulo di documentazione interna della violazione da inviare all'indirizzo dedicato databreachuda@pec.unich.it, che deciderà se attivare o meno il Team di risposta inoltrando la relativa segnalazione.
- area informatica mediante opportuni strumenti di monitoraggio ed analisi di eventi di natura *software* e ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dai sistemi di security ICT dell'Ateneo. Tali eventi relativi ai sistemi ICT sono di responsabilità e conseguentemente monitorati e gestiti dall'Area Informatica e dagli Amministratori di Sistema opportunamente incaricati. In caso di concreta, potenziale o meramente sospetta violazione di dati personali, la suddetta Area deve **immediatamente** informare il Titolare mediante la compilazione dell'**Allegato 1 (Modulo di documentazione interna della violazione**) da inviare all'indirizzo databreachuda@pec.unich.it.

B) **Canali esterni**

Le segnalazioni di eventi anomali possono pervenire anche dell'esterno:

- segnalazione da parte dell'interessato o di terzi: l'interessato (ad es. studenti, docenti, dipendenti, ecc) o eventuali terzi, possono effettuare una segnalazione anche in caso di semplice sospetto che i propri dati personali siano stati utilizzati in maniera fraudolenta da terzi o in generale che siano stati oggetto di violazione mediante compilazione del modulo dedicato (Allegato 1 – Modulo di documentazione interna della violazione di dati personali). In questi casi, l'interessato potrà rivolgersi al Titolare o all'RPD dell'Organizzazione (che attiverà prontamente il Titolare) per la segnalazione di eventuali violazioni secondo quanto disposto dalla specifica informativa (**Allegato 2 – Informativa sul trattamento dei dati personali relativa alla segnalazione di Data Breach**) relativa segnalazione di Data Breach pubblicata sul sito https://www.unich.it/privacy.

- segnalazione dal responsabile (esterno) del trattamento: il responsabile del trattamento, in caso di concreta, potenziale o meramente sospetta violazione di dati personali, deve immediatamente informare il Titolare, mediante la compilazione dell'Allegato 1 - Modulo di documentazione interna della violazione da inviare all'indirizzo dedicato databreachuda@pec.unich.it, che deciderà se attivare il Team di risposta, inoltrando la relativa documentazione ricevuta.

7.2 Gestione della violazione (valutazione e decisione)

La gestione di una violazione di dati personali è stata standardizzata in un processo suddiviso nelle seguenti cinque fasi:

a) Ricezione segnalazione e prima sommaria valutazione del Titolare;
b) analisi preliminare delle segnalazioni (Team di risposta alle violazioni) ed eventuale annotazione nel registro ufficiale da parte dell'Ufficio Privacy;
c) *risk assessment* e individuazione delle misure da adottare;
d) eventuale notifica al Garante per la protezione dei dati personali
e) eventuale comunicazione agli interessati

7.2.1 Ricezione segnalazione e prima sommaria valutazione del Titolare (Titolare)

Ricevuta notizia di un possibile *data breach* il Titolare, dopo una prima sommaria valutazione, decide se attivare il team di risposta o se, in presenza di un palese "falso positivo", sentito il parere dell'RPD disporre l'archiviazione della segnalazione. In caso di eventuale dissenso con l'RPD il Titolare potrà decidere se attivare il Team di risposta o se procedere comunque ad archiviazione, documentando l'eventuale dissenso dell'RPD.

7.2.2 Analisi preliminare delle segnalazioni (Team di risposta alle violazioni)

La struttura incaricata della valutazione approfondita delle segnalazioni di violazioni di dati personali è il Team di risposta alle violazioni. Questo effettuerà – anche con la collaborazione del Responsabile della protezione dei dati personali, che sarà prontamente coinvolto a seguito della ricezione della segnalazione dell'anomalia di cui al par. 7.1. che precede - un'analisi preliminare ulteriore rispetto a quella già preliminarmente effettuata dal Titolare, alla luce delle competenze di tutti i componenti il team e sentito l'RPD, sulle base delle informazioni relative alla presunta violazione raccolte attraverso l'Allegato 1 - Modulo di documentazione interna della violazione.
A seguito della ricezione della segnalazione da parte del Titolare, il Team di risposta con il supporto dell'Ufficio Privacy compila eventualmente l'Allegato 1 - Modulo di documentazione interna della violazione fornendo ogni ulteriore elemento utile al fine di una seconda valutazione di maggior dettaglio. Successivamente il legale rappresentante del Titolare del trattamento (membro del Team), sentito il parere del Responsabile della protezione dei dati personali (in caso di parere discordante da parte dell'RPD questo andrà documentato annotandolo nel registro dei data breach dal Titolare), effettuerà, alla luce di eventuali nuovi elementi emersi dal lavoro istruttorio del Team, una seconda valutazione preliminare riguardante la possibile violazione occorsa, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di violazione e se sia necessaria un'indagine più approfondita e strutturata dell'accaduto. Il questo secondo caso il Titolare attiverà il Team che avvierà la fase di *risk assessment* coinvolgendo, con ruolo consultivo, l'RPD. Nel caso in cui l'evento venga accertato come "falso positivo", la procedura di verifica verrà chiusa e l'evento verrà archiviato.

Nel caso in cui la violazione venga accertata e si ritenga di trovarsi di fronte ad un Data Breach, il Team di riposta procede al recupero di quante più informazioni possibili relative alla violazione per la gestione dell'evento e dispone l'inserimento, con numero progressivo, del Data breach nell'apposito elenco.

Al fine di una migliore istruttoria in termini di impatto per i soggetti interessati, le valutazioni dovranno tenere conto di tali eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale o di dati giudiziari;
b) che si tratti di dati relativi a 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;
c) che si tratti di dati relativi a persone fisiche vulnerabili, quali ad esempio minori;
d) che il trattamento riguardi una notevole quantità di dati personali;
e) che il trattamento riguardi un vasto numero di interessati.

7.2.2.1 Azioni di contenimento

Alcune *best practices* da attuare in caso di violazione di dati personali sono quelle elencate di seguito. Si precisa che si tratta di un elenco meramente esemplificativo e non esaustivo e che resta ferma la necessità di operare una valutazione caso per caso.

a) contenere i dispositivi infettati mettendoli *off-line*;
b) censire le macchine che sono state violate;
c) individuare quali vulnerabilità sono state sfruttate per violare le macchine ed eventualmente gli apparati di rete;
d) raccogliere evidenze per il Garante per la protezione dei dati personali, in modo tale da dimostrare quali misure siano state impiegate e quali azioni siano state attuate durante l'evento cibernetico;
e) ripristinare i sistemi e le reti;
f) integrare le informazioni raccolte per individuare nuove misure al fine di stabilire un nuovo piano per far sì che l'incidente non si ripeta in futuro.

7.2.3 Risk *assessment* e individuazione delle misure

Al termine della fase di valutazione preliminare, nel caso si accerti una reale violazione, il Team di risposta, sentito il Responsabile della protezione dei dati personali, stabilisce:

a) le opportune misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare (ad es.: riparazione fisica di strumentazione; utilizzo dei *file* di *back-up* per recuperare dati persi o danneggiati; isolamento o chiusura di un settore compromesso della rete; cambio dei codici di accesso, ecc.);
b) le modalità e le tempistiche di suddette misure, individuando gli attori e i compiti per limitare la violazione;
c) se la violazione ricade nei casi in cui è necessario effettuare la notifica al Garante per la Protezione dei dati personali;

d) se la violazione ricade nei casi in cui è necessario informare dell'accaduto l'interessato o gli interessati coinvolti nella violazione.

Al fine di individuare la necessità di notifica al Garante per la protezione dei dati personali e di comunicazione agli interessati, il Team, sentito il parere del Responsabile per la protezione dei dati, valuterà la gravità della violazione utilizzando un modello standardizzato (**Allegato 3 – Modello di valutazione della segnalazione**). In caso di eventuale dissenso con l'RPD questo andrà documentato.

Si precisa che gli obblighi di notifica al Garante scaturiscono dal superamento di una soglia di rischio tale da essere **non trascurabile**; mentre l'art. 34 del Regolamento prevede che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio **elevato**.

7.2.4 Notifica al Garante

Se a seguito delle valutazioni preliminari e del *risk assessment*, effettuati nel rispetto delle indicazioni operative sin qui descritte, dovesse emergere la necessità di effettuare la notifica della violazione di dati al Garante, il Titolare del trattamento, sentito il parere del Responsabile della protezione dei dati personali, provvederà alla notifica, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021).

Procedura per la gestione delle violazioni di dati personali

La notifica al Garante per la protezione dei dati personali deve (almeno):

a) descrivere la natura della violazione di dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, 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 di 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.

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

Comunque la segnalazione sarà effettuata dal Titolare o da suo delegato per mezzo della citata procedura telematica dedicata, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

7.2.5 Comunicazione agli interessati

Se a seguito delle valutazioni preliminari e del *risk assessment*, effettuati nel rispetto delle indicazioni operative sin qui descritte, è stata valutata la necessità di effettuare la comunicazione della violazione di dati agli interessati, il Titolare del trattamento, sentito il parere del Responsabile della protezione dei dati personali, provvederà alla comunicazione senza ingiustificato ritardo agli stessi. In caso di eventuale dissenso con l'RPD questo andrà opportunamente documentato.

La comunicazione agli interessati, che dovrà essere effettuata tramite una modalità diretta (ad es. tramite e-mail o p.e.c.) deve (almeno):

a) indicare il nome e i dati di contatto del Responsabile della protezione dei dati personali;
b) contenere la descrizione delle probabili conseguenze della violazione di dati personali;
c) contenere la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Nei seguenti casi **non è richiesta** la comunicazione all'interessato:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure sono 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 (ad es. 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 par. 1 dell'art. 34 del Regolamento;
c) nel caso in cui detta comunicazione dovesse richiedere sforzi sproporzionati. In tal caso, si procederà con una comunicazione pubblica o similare, tramite la quale gli interessati siano informati con analoga efficacia.

7.3 Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere alla notifica o alla comunicazione della violazione, ogni qualvolta si verifichi un incidente, l'Università sarà tenuta a documentarlo.

La documentazione relativa alle violazioni di dati personali sarà conservata dal Titolare del trattamento dei dati presso l'ufficio Privacy.

Il Titolare del trattamento, rendendo disponibile la consultazione al Responsabile per la protezione dei dati ogni qual volta ciò si rendesse necessario, provvederà alla tenuta di un apposito registro delle violazioni, in cui saranno riportate le seguenti informazioni:

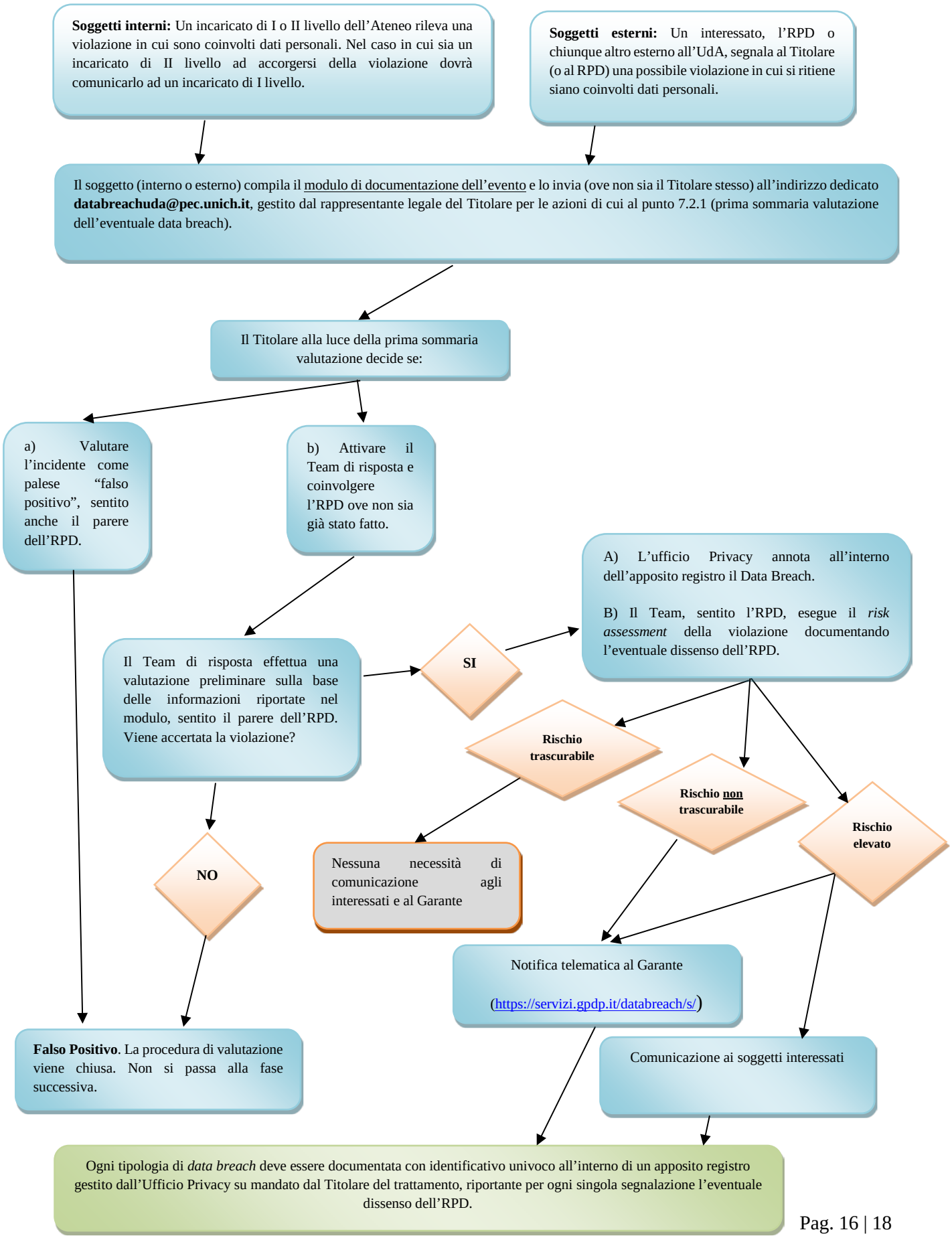
a) numero della segnalazione;
b) data della segnalazione;
c) dati identificativi del segnalatore;
d) sintesi della valutazione effettuata;
e) indicazione dell'eventuale notifica effettuata al Garante per la protezione dei dati personali;
f) indicazione dell'eventuale comunicazione effettuata agli interessati;
g) Eventuale parere discordante dell'RPD.

Il registro delle violazioni (il cui modello è indicato nell'Allegato 2 al presente documento) sarà costantemente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi, mediante l'applicazione GDP – Gestione Normativa GDPR, del CINECA di Casalecchio di Reno, Bologna.

7.4 Analisi post-violazione

Dopo aver posto in essere le sin qui indicate attività, è necessaria la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione

dell'evento ed identificare possibili aree di miglioramento che svilupperanno ulteriormente l'efficacia del piano di gestione delle violazioni, quale considerato nel suo complesso. Tale attività sarà posta in essere dal Team di risposta alle violazioni con il supporto del Responsabile per la Protezione dei Dati.


Soggetti interni: Un incaricato di I o II livello dell'Ateneo rileva una violazione in cui sono coinvolti dati personali. Nel caso in cui sia un incaricato di II livello ad accorgersi della violazione dovrà comunicarlo ad un incaricato di I livello.
Soggetti esterni: Un interessato, l'RPD o chiunque altro esterno all'UdA, segnala al Titolare (o al RPD) una possibile violazione in cui si ritiene siano coinvolti dati personali.
Il soggetto (interno o esterno) compila il modulo di documentazione dell'evento e lo invia (ove non sia il Titolare stesso) all'indirizzo dedicato **databreachuda@pec.unich.it**, gestito dal rappresentante legale del Titolare per le azioni di cui al punto 7.2.1 (prima sommaria valutazione dell'eventuale data breach).
Il Titolare alla luce della prima sommaria valutazione decide se:
a) Valutare l'incidente come palese "falso positivo", sentito anche il parere dell'RPD.
b) Attivare il Team di risposta e coinvolgere l'RPD ove non sia già stato fatto.
Il Team di risposta effettua una valutazione preliminare sulla base delle informazioni riportate nel modulo, sentito il parere dell'RPD. Viene accertata la violazione?
SI
A) L'ufficio Privacy annota all'interno dell'apposito registro il Data Breach.
B) Il Team, sentito l'RPD, esegue il *risk assessment* della violazione documentando l'eventuale dissenso dell'RPD.
Rischio trascurabile
Rischio non trascurabile
Rischio elevato
NO
Nessuna necessità di comunicazione agli interessati e al Garante
Notifica telematica al Garante
(https://servizi.gpdp.it/databreach/s/)
Falso Positivo. La procedura di valutazione viene chiusa. Non si passa alla fase successiva.
Comunicazione ai soggetti interessati
Ogni tipologia di *data breach* deve essere documentata con identificativo univoco all'interno di un apposito registro gestito dall'Ufficio Privacy su mandato dal Titolare del trattamento, riportante per ogni singola segnalazione l'eventuale dissenso dell'RPD.

8 *Data breach* presso l'Ateneo quando opera in qualità di responsabile (esterno) del trattamento

8.1 Obblighi di comunicazione dell'Università quando opera in qualità di responsabile

Quando l'Università agisce in qualità di responsabile (esterno) del trattamento, in caso di violazione di dati personali, deve informare il titolare del trattamento senza ingiustificato ritardo secondo i tempi e i modi con questi concordati nell'atto di designazione quale responsabile del trattamento o in qualsiasi atto disciplinante il rapporto instaurato.

9 Allegati

- **Allegato 1 - Modulo di documentazione interna della violazione della violazione dei dati personali**
- **Allegato 2 - Modello di registro segnalazioni per le violazioni**
- **Allegato 3 - Modello di valutazione della segnalazione**
- **Allegato 4 – Recapiti e nominativi dei componenti del Data Breach Response Team - DBRT**