Allegato 1 – Data breach

Scopo del presente documento è fornire delle linee guida operative per la gestione de Processo per l'analisi ed identificazione di un eventuale Data Breach e la gestione dell'eventuale notifica delle violazioni dei dati personali al Garante Privacy e, qualora necessario/richiesto, agli interessati in conformità a quanto disposto dal Regolamento (UE) 2016/679 e in particolare in conformità alle Linee Guida WP250 adottate il 3 ottobre 2017 e redatte dal Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art. 29 della Direttiva Europea 95/46[1].
Notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679

Il Data Breach e gli adempimenti correlati

L'art. 4 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (da ora in avanti anche "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, sancisce che una violazione dei dati personali ("Data Breach") è "*una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Il Gruppo di lavoro dei Garanti Europei, con le linee guida WP250, ha meglio precisato che i Data Breach sono classificabili in tre macro-categorie:

- ✓ "Confidentiality Breach", quando vi è un accesso accidentale o abusivo a Dati personali;
- ✓ "Availability Breach", quando vi è una perdita o distruzione accidentale o non autorizzata del Dato personale;
- ✓ "Integrity Breach", quando vi è un'alterazione accidentale o non autorizzata del Dato personale.

Sono stati forniti alcuni esempi significativi di data breach che possono essere di grande utilità per inquadrare il contesto con particolare riferimento al caso di "Avaibility Breach".

Perdita di un device non cifrato	Anche il semplice smarrimento di uno smartphone può costituire una valida ragione di un data breach nel caso in cui contenga Dati personali e non sia stato opportunamente cifrato.
Perdità di disponibilità del Dato personale	Un esempio potenziale di perdita di disponibilità del dato è quando un Dato personale viene inviato per errore ad un terzo non autorizzato.

Per un'analisi più approfondita di possibili esempi di Data Breach si rimanda al paragrafo a pagina 12.

Tipologie di Data Breach

Gli eventi che possono causare un Data Breach sono così raggruppati nell'articolo 4 (12) del GDPR sulla base delle linee guida ENISA:

- Unauthorized Access: accesso ai dati da parte di soggetti (interni o esterni) non aventi diritto.
- Loss: indisponibilità temporanea dei dati.
- Destruction: indisponibilità irreversibile dei dati.
- Transmission: comunicazione (fortuita o intenzionale) dei dati verso terzi non autorizzati.
- Alteration or Modification: modifica impropria (accidentale o intenzionale) dei dati.
- Disclosure: divulgazione impropria di informazioni riservate.

[1] WP 250 rev.01 – *Guidelines on Personal Data Breach Notification Under Regulation 2016/679* (Documento del Working Party Art. 29 adottato il 6 febbraio 2018). Si suggerisce la lettura dei seguenti documenti:

- WP248. Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017.
- Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).*
- European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*

Notifica al Garante per la Protezione dei Dati Personali (ex art. 33 del GDPR)

Il disposto normativo GDPR, ai sensi dell'articolo 33, ha inoltre previsto fra gli ulteriori adempimenti in capo a tutte le organizzazioni che trattano dati personali, l'obbligo di notifica dell'avvenuta violazione dei dati personali al Garante per la Protezione dei Dati Personali; la notifica deve avere i seguenti requisiti:

- ✓ descrivere la natura della violazione dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione;
- ✓ comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- ✓ descrivere le probabili conseguenze della violazione dei Dati personali;
- ✓ 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 notifica deve essere effettuata entro 72 ore e senza "ingiustificato ritardo", da quando il Titolare è venuto a conoscenza del Data Breach. L'art. 33, comma 3 del GDPR chiarisce inoltre che quando non è possibile fornire tutte le informazioni nello stesso momento si può procedere all'invio delle informazioni mancanti in una fase successiva. Infine, può anche accadere che il Titolare del Trattamento notifichi la perdita della disponibilità di un determinato supporto al Garante per la Protezione dei Dati Personali che in un momento successivo lo ritrovi all'interno dei propri uffici senza che lo stesso sia stato alterato. In questo caso, è sufficiente comunicare all'Autorità che il supporto è stato ritrovato e richiedere che la procedura di notifica venga annullata.

Notifica agli Interessati (ex art.34 del GDPR)

Nel caso in cui la violazione dei Dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il GDPR obbliga il Titolare del Trattamento a comunicare tale violazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi Dati personali.

La comunicazione del Data Breach all'Interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei Dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi Dati personali. Tuttavia, si può essere esonerati dalla notifica all'Interessato, ove:

- ✓ 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;
- ✓ 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;
- ✓ la 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;
- ✓ i contenuti delle comunicazioni violate sono interamente cifrati.

Registro dei Data Breach

Ai sensi dell'art. 33 del GDPR è obbligatorio per il Titolare del Trattamento conservare la documentazione attestante tutti i Data Breach avvenuti. Il Titolare conserva, quindi, un registro dei Data Breach che deve essere tempestivamente aggiornato e contenere le seguenti informazioni:

- ✓ i dettagli relativi al Data Breach (e cioè la causa, il luogo dove è avvenuto e la tipologia di Dati personali violati);
- ✓ gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal Titolare.

Oltre a questi aspetti, il Titolare dovrebbe anche motivare la ragione delle decisioni assunte a seguito del Data Breach con particolare riferimento ai seguenti casi:

- ✓ il Titolare ha deciso di non procedere alla notifica;
- ✓ il Titolare ha ritardato nella procedura di notifica;
- ✓ il Titolare ha deciso di non notificare il Data Breach agli Interessati.

Concetti chiave

Il Data Breach è una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	La notifica deve essere effettuata entro 72 ore e senza "ingiustificato ritardo", da quando il Titolare è venuto a conoscenza del Data Breach. In caso di particolare complessità il Titolare può fornire ulteriori dettagli del Data Breach successivamente ("notifica preliminare").
Nel caso in cui il Data Breach sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il GDPR obbliga il Titolare del Trattamento a comunicare tale violazione anche a ciascun Interessato.	Ai sensi dell'art. 33 del GDPR è obbligatorio per il Titolare del Trattamento conservare la documentazione attestante tutti i Data Breach avvenuti attraverso il registro degli incidenti informatici.

Procedura notifica di Data Breach

La procedura di notifica di una Data Breach viene avviata ogni qualvolta il Titolare dei dati, un ConTitolare dei dati, un Responsabile/Designato del Trattamento, un Incaricato al trattamento, un Interessato, identifichi o venga informato di una violazione di sicurezza che possa comportare 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 (Data Breach).

La procedura deve essere avviata senza indugio e conclusa nel più breve tempo possibile. Ogni qualvolta la procedura viene avviata, deve essere effettuata apposita registrazione dell'evento nel registro dei Data Breach dell'Ateneo.

Il modulo di segnalazione del Data Breach

La segnalazione di un incidente con potenziale Data Breach viene effettuata scrivendo alla casella e-mail istituita da Sapienza a tale scopo. Tale modulo potrà essere personalizzato sulla base dell'esigenze di ogni singolo Ateneo e sulla base dell'esperienza maturata negli anni. Alcune domande, infatti, potrebbero non essere di immediata comprensione per un soggetto non particolarmente competente in materia di protezione dei dati personali. Di seguito si riportano le domande che potrebbero essere rivolte:

1	Dati di contatto di chi effettua la segnalazione
2	Quando è avvenuta o è venuto a conoscenza della violazione?
3	Classificazione dell'incidente
4	Possibili cause della violazione delle proprie credenziali
5	Ha provveduto ad azioni per limitare i danni e se si, quali?
6	Tipologia dei dati coinvolti
7	Categorie dei dati coinvolti
8	Tipo di violazione sui dati

La valutazione della gravità della violazione di dati personali

Il Titolare valuta il livello di gravità di una violazione di dati personali rispetto ai diritti e alle libertà dei soggetti interessati. Potrebbe essere necessario effettuare più valutazioni in tempi diversi, in base alle informazioni raccolte anche durante le fasi successive.

I principali parametri da tenere in considerazione durante la valutazione dell'impatto di una violazione di dati personali sono i seguenti:

- ✓ il Contesto del trattamento dei dati (Data Processing Context - DPC): tiene conto della natura dei dati oggetto della violazione, insieme ad altri fattori relativi al contesto generale del trattamento dei dati;
- ✓ la Facilità di Identificazione (Ease of Identification - EI): stima di quanto sia facile identificare i soggetti interessati a partire dai dati oggetto della violazione;
- ✓ le Circostanze della violazione (Circumstances of breach - CB): prende in considerazione le circostanze specifiche della violazione, relative alla sua tipologia, contemplando la perdita di sicurezza dei dati e gli eventuali scopi malevoli connessi.

Dopo aver completato l'analisi preliminare sull'effettivo rischio per i diritti degli interessati e dopo aver iniziato l'inserimento dell'evento nel registro degli incidenti informatici, ove le risultanze dell'analisi non diano un esito basso, deve essere avviata la seguente procedura della notifica del Data Breach nei tempi indicati dalla normativa (72 ore dall'avvenuta conoscenza del Breach) secondo il modello pubblicato sul sito web dell'Autorità.

Di seguito vengono riportate le domande alle quali si dovrà dare risposta per la corretta compilazione della notifica. Per ogni domanda verranno riportate delle sintetiche indicazioni operative e, ove presenti, le linee guida del Gruppo "Articolo 29" e dell'Autorità Garante per la Protezione dei dati personali a cui si dovrà fare riferimento in caso di dubbio interpretativo.

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

In risposta a questa prima domanda, deve essere fornita una breve descrizione dell'incidente occorso indicando le banche dati oggetto di violazione. Può accadere che il tipo di incidente abbia un grado di complessità particolarmente elevato. A tal proposito si ricorda che ai sensi dell'art. 33, comma 4, del GDPR "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".
Sotto un profilo operativo, deve essere attentamente valutata, in taluni casi di particolare complessità e che potrebbero avere anche una rilevanza penale, la possibilità di coinvolgere un consulente informatico al fine di garantire l'acquisizione, nel rispetto delle best practices della digital forensics, delle prove digitali idonee a dimostrare la violazione dei dati occorsa.

2	Quando si è verificata la violazione dei dati personali?

Il Gruppo di lavoro ritiene che il Titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Tuttavia, il considerando 87 del GDPR chiarisce che il Titolare del trattamento è tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate. Per questa ragione, ove si notificasse una violazione decorse le 72 ore previste è importante chiarire le ragioni per cui non sia stato possibile venirne a conoscenza prima.
Il Gruppo "Articolo 29" ha fornito 4 utili esempi per comprendere quando il Titolare del trattamento può ritenere di essere venuto a conoscenza della violazione che si riportano:

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il Titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il Titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.
2. Un terzo informa il Titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al Titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".
3. Un Titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il Titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.
4. Un criminale informatico viola il sistema del Titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il Titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

3	Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

In alcuni casi è particolarmente complesso determinare il luogo dove è avvenuta la violazione. Ad esempio, quando vi è un accesso accidentale o abusivo a dati personali (confidentiality breach) avvenuto su server cloud o qualora non sia stato possibile identificare le modalità con cui si è verificata la potenziale perdita di confidenzialità delle credenziali, diventa difficile identificare il dispositivo oggetto di violazione.
In tali casi, è necessario cristallizzare, nel rispetto delle best practices della digital forensics, la prova digitale al fine di poter fornire tutti gli elementi utili a ricostruire l'accaduto, nel caso in cui il Garante per la Protezione dei Dati Personali dovesse richiedere ulteriori chiarimenti a seguito della violazione.
Nel caso di smarrimento di dispositivi o di supporti portatili, invece, si ricorda che è necessario denunciare il fatto presso l'autorità giudiziaria e, ove tecnicamente possibile, effettuare da remoto la cancellazione dei dati presenti nel dispositivo.

4	Modalità di esposizione al rischio Tipo di violazione e dispositivo oggetto della violazione

I tipi di violazione possono essere i seguenti: lettura, copia, alterazione, cancellazione, furto. Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.
Il Gruppo "Articolo 29" porta due esempi che possono essere utili a valutare il tipo di violazione. Nel primo, si può avere perdita di disponibilità quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il Titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente. Nel secondo esempio, può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (denial of service) che rende i dati personali indisponibili. Va notato, infine, che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il Titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi. Ad esempio, un'infezione da ransomware (software dannoso che cifra i dati del Titolare del trattamento finché non viene pagato un riscatto) potrebbe comportare una perdita temporanea di disponibilità se i dati possono essere ripristinati da un backup. Tuttavia, si è comunque verificata un'intrusione nella rete e potrebbe essere richiesta una notifica se l'incidente è qualificato come violazione della riservatezza (ad esempio se chi ha effettuato l'attacco ha avuto accesso a dati personali) e ciò presenta un rischio per i diritti e le libertà delle persone fisiche. Per quanto attiene l'indicazione del dispositivo oggetto della violazione valgano le considerazioni sopra svolte in tema di ubicazione. Non sempre è possibile identificare il dispositivo oggetto della violazione, ma è sicuramente opportuno dimostrare di aver attuato un sistema di gestione delle violazioni del dato personale efficiente e funzionale allo scopo.

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

Questa domanda può generare non pochi problemi nel caso in cui la violazione sia dovuta ad un attacco informatico su un numero particolarmente elevato di dispositivi. In tal caso, la descrizione sintetica potrebbe essere fatta per categorie di sistemi di elaborazione o memorizzazione coinvolti. In casi di particolare complessità, si ricorda la possibilità di effettuare la notifica per "fasi" ai sensi dell'art. 33, comma, 4 del GDPR.

6	Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

Il Gruppo Articolo 29 chiarisce che la mancanza di disponibilità di informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per "fasi".

7	Che tipo di dati sono oggetto di violazione?

I dati che potrebbero essere oggetto di violazione possono essere dati comuni o rientrare nelle categorie particolari di dati elencate nel modulo di notifica della violazione dei dati personali. Il GDPR non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo "Articolo 29" suggerisce di indicare le categorie di registrazioni dei dati personali che il Titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.
Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

8	Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del Titolare)

I considerando 75 e il 76 del GDPR ben sintetizzano il concetto di rischio chiarendo che "i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: 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". Sulla base di tali parametri è possibile giudicare basso/trascurabile, medio, medio alto e alto il livello di rischio che dovrà considerare anche i seguenti fattori:

- Tipo di violazione
- Natura, carattere sensibile e volume dei dati personali
- Facilità di identificazione delle persone fisiche
- Gravità delle conseguenze per le persone fisiche
- Caratteristiche particolari dell'interessato
- Caratteristiche particolari del Titolare del trattamento di dati
- Numero di persone fisiche interessate

Le Linee Guida del WP29 sul Data Breach chiariscono che, nel valutare il rischio che potrebbe derivare da una violazione, il Titolare del trattamento dovrebbe considerare, oltre che la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche, anche la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio.

9	Misure tecniche e organizzative applicate ai dati oggetto di violazione

A questo quesito è necessario rispondere con l'elencazione delle misure tecniche e organizzative esistenti al momento della violazione.

Il GDPR prevede chiaramente che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Di conseguenza, si impone tanto al Titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (art. 33, comma 1).

10	La violazione è stata comunicata anche agli interessati?

Il Titolare del trattamento deve tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Si ricorda che il GPDR all'art. 34, comma 3 stabilisce che non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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

Il paragrafo 5 delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il Titolare del trattamento deve comunicarla agli interessati.

11	Qual è il contenuto della comunicazione resa agli interessati?

Il Titolare del trattamento deve fornire in modo assolutamente semplice e chiaro le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il Titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il Titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il Titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato, salvo i residuali casi previsti dall'art. 34 comma 3. Il Gruppo di lavoro raccomanda al Titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il Titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.

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

Questo quesito è sicuramente uno dei più importanti e necessità di una risposta sicuramente sintetica, ma quanto mai efficace. È evidente che, una volta verificatosi una violazione, il c.d. "piano rimediale" è fondamentale per garantire la tutela degli interessati che l'hanno subita. Sotto questo profilo si suggerisce di proporre un piano che si fondi su tre parametri molto noti nel settore sicurezza informatica: formazione ("people"), procedure e processi ("process") e tecnologia ("techonology"). Il fatto che l'implementazione delle misure tecnologiche sia messo al terzo posto non è casuale: infatti, le misure di sicurezza tecnologiche possono essere parzialmente utili se le persone non rispettano le regole previste dalle procedure o se addirittura tali regole non sono presenti. Per questa ragione, la conoscenza, il rispetto e il costante aggiornamento del regolamento dell'Ateneo sulle risorse informatiche aziendali è di fondamentale importanza.

Da ultimo, si segnala che, nell'ambito della notifica all'autorità di controllo, il Titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

Esempi di Data Breach

Per meglio contestualizzare il riconoscimento dei Data Breach in Sapienza, di seguito vengono proposti alcuni casi a titolo esemplificativo ma non esaustivo basati su quelli proposti dal Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art.29 della Direttiva Europea 95/46:

Tipologia Data Breach	Esempio	Necessita Notifica la Garante Privacy?	Necessita Notifica agli interessati?	Note
Availability Breach	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati non cifrati o cifrati con algoritmi non allo stato dell'arte.	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Availability Breach	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati cifrati con algoritmi allo stato dell'arte.	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Confidentiality Breach	Una applicazione informatica subisce un attacco informatico a fronte del quale gli attaccanti hanno avuto accesso a dati personali e c'è il ragionevole sospetto che li abbiano consultati e/o sottratti (esempi di applicativi: Gestione Documentale, Gestione carriera studenti, Gestione del personale Ugov Risorse Umane, Gestione Diritto allo studio, Gestione prestito bibliotecario, Servizio di Posta Elettronica Office 365, etc.).	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Availability Breach	Temporanea non disponibilità di un server, un applicativo o della connettività di rete (ad esempio per mancanza energia elettrica, guasto degli apparati).	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Confidentiality Breach/Availability Breach	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, non esiste un BackUp dei dati e/o c'è una ragionevole evidenza che i dati personali possono essere stati esfiltrati dal dispositivo.	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach/Availability Breach	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, esiste un BackUp dei dati per cui possono essere ripristinati in tempi ragionevoli e c'è una ragionevole evidenza che i dati personali non sono stati sottratti dal dispositivo.	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach

Tipologia Data Breach	Esempio	Necessita Notifica la Garante Privacy?	Necessita Notifica agli interessati?	Note
Confidentiality Breach	Un Titolare di credenziali di accesso a sistemi informatici che trattano dati personali segnala una perdita di confidenzialità delle proprie credenziali (ad esempio per aver dato seguito ad un messaggio di Phishing), da una veloce investigazione risulta che le credenziali siano state usate per accedere a dati personali con attività non riconducibili all'utente autorizzato.	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	A seguito di un attacco informatico sono state trafugate le credenziali di utenze con privilegi di accesso a dati personali, tali credenziali erano memorizzati sul server in modalità non cifrata o cifrate con algoritmi non allo stato dell'arte o con meccanismi di cifratura non reversibile (hash) non allo stato dell'arte.	SI	SI	
Confidentiality Breach	A seguiti di un errore di programmazione e configurazione di un sistema informatico o di una applicazione informatica, sono stati resi accessibili dati personali a soggetti non Autorizzati al trattamento o diversi dagli Interessati, inoltre da una rapida investigazione risulta che sono stati fatti accessi in violazione di quanto sopra.	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Comunicazione di dati personali ad errato destinatario (ad esempio per invio ad indirizzo email errato).	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Invio a mailing list di uno o più messaggi con gli indirizzi email dei destinatari in chiaro nel campo 'A' o nel campo 'CC'.	SI se l'evento coinvolge un largo numero di individui	Dipende dallo scopo e dalla finalità della mailing list	