DATA BREACH: PIANO DI SICUREZZA e PROCEDURA OPERATIVA

Regolamento UE 2016/679 in materia di protezione dei dati personali

Premessa

Il presente documento è redatto a cura del gruppo di supporto al RPD (DR n. 332/2018, prot n. 44955), con la consulenza del RPD stesso, e viene aggiornato con cadenza annuale.

Una violazione dei dati personali (cosiddetto «*data breach*») consiste in 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» (Art. 4, definizione 12)

La violazione può essere determinata da accesso abusivo ai sistemi informatici, ovvero da sottrazione o perdita di dati e supporti di memorizzazione.

Il Titolare deve notificare alle Autorità Garanti, senza ingiustificato ritardo (e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza) eventuali violazioni dei dati e comunicarle agli interessati senza ingiustificato ritardo, laddove vi sia un rischio elevato per i diritti e le libertà delle persone fisiche (art. 33).

La notifica all'Autorità deve, fra l'altro, descrivere:

- la natura della violazione dei dati personali;
- ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- 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.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, al fine di consentire all'autorità di controllo di verificare il rispetto di quanto previsto nell'art. 33. Per i dati trattati dai soggetti terzi, il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Il titolare è tenuto a documentare il modo in cui viene a conoscenza della violazione. Ritardi nell'individuazione del data breach, dovute a carenza di misure tecniche e organizzative, o ad omessi controlli interni, costituiscono elementi che il Garante può vagliare in sede di provvedimenti o di eventuali misure sanzionatorie.

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 è tenuto a comunicare la violazione all'interessato senza ingiustificato ritardo (art. 34). Tale comunicazione è volta a ridurre il danno che può derivare all'interessato in conseguenza della violazione (consentendogli di adottare contromisure idonee a contenere gli effetti dannosi della violazione). La comunicazione all'interessato non è richiesta se erano state applicate ai dati oggetto della violazione adeguate misure di sicurezza destinate a rendere i dati

personali incomprensibili (quali la cifratura) oppure se sono successivamente adottate misure atte a scongiurare un rischio elevato. La valutazione sulla necessità della comunicazione è in capo al titolare, anche se l'Autorità può obbligarlo ad effettuarla nel caso in cui non l'avesse ritenuta necessaria.

Misure di sicurezza – riduzione preventiva del rischio

L'Ateneo ha adottato un insieme di regolamenti, volti a prevenire i rischi di data breach (vedi Normativa di Ateneo - Regolamenti area informatica):

- Accesso al Sistema Integrato di Reti dell'Ateneo - SIRA
- Regolamento in materia di utilizzo della posta elettronica e della rete internet messi a disposizione dall'Università di Trieste
- Regolamento per i servizi web di Ateneo

Il presente piano di gestione della sicurezza è pubblicato nella pagina *Sicurezza informatica* presente nella sezione *intranet* del portale di Ateneo.

Il personale dell'Ateneo viene sensibilizzato sul tema della sicurezza informatica attraverso periodici appuntamenti formativi ed attraverso una pagina dedicata presente sul portale di Ateneo in *intranet, Sicurezza informatica* e può contare sull'indirizzo mail di supporto sicurezzainformatica@units.it.

Con cadenza annuale l'Ateneo aggiorna il rapporto relativo ai controlli previsti dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni", in ottemperanza a quanto previsto dalla circolare 18 aprile 2017, n. 2/2017 dall'AGID – Agenzia per l'Italia Digitale:

- analisi e ricognizione della situazione attuale in termini di architettura hardware e software
- elenco dei software autorizzati e regolamenti operativi in tal senso
- esecuzione periodica di scansioni sui sistemi per la rilevazione di software non autorizzato/aggiornato
- definizione configurazioni sicure standard per la protezione dei sistemi operativi
- verifica e certificazione che le operazioni di amministrazione di sistema remote di server, workstation e dispositivi di rete siano effettuate per mezzo di connessioni sicure
- scansione di vulnerabilità ai sensi del punto 4.1.1 della circolare AGID
- limitazione dei privilegi di administrator ai soli utenti che abbiano competenze adeguate e la necessità operativa dimostrabile di modificare la configurazione dei sistemi
- censimento account di administrator
- individuazione e inventariazione dei soggetti che operano con qualifica o comunque profilo di administrator
- nomina ad amministratore di sistema (soggetti sia interni che esterni)

I controlli sono descritti ed eseguiti dalle strutture dell'Area dei Servizi ICT per l'Amministrazione Centrale ed i sistemi gestiti centralmente, nonché dai Direttori di Dipartimento e dal Settore Servizi per il Trasferimento delle Conoscenze – SBA per i sistemi periferici.

Anche in base all'esito dei controlli di cui sopra, vengono aggiornate con continuità le configurazioni dei dispositivi hardware ed i sistemi software rivolti a ridurre i rischi informatici (firewall perimetrali, dispositivi di accesso VPN, antispam ed antivirus per postazioni di lavoro e posta elettronica, misure

infrastrutturali di isolamento fisico e logico di determinate categorie di dispositivi, dispositivi di backup, sistemi di cifratura e pseudonimizzazione, ecc…)

Ad opera delle strutture dell'Area dei Servizi ICT, prima fra tutte l'Ufficio Reti di Ateneo, con cadenza almeno semestrale, vengono eseguite scansioni sull'intera infrastruttura di rete di Ateneo, utilizzando sistemi di vulnerability assessment, per rilevare programmi e sistemi operativi non aggiornati o non più supportati. Tali vulnerabilità sono riportate ai rispettivi amministratori.

Specifici canali e modalità di comunicazione sono adottati per inviare e ricevere notifiche riguardo le problematiche di sicurezza informatica:

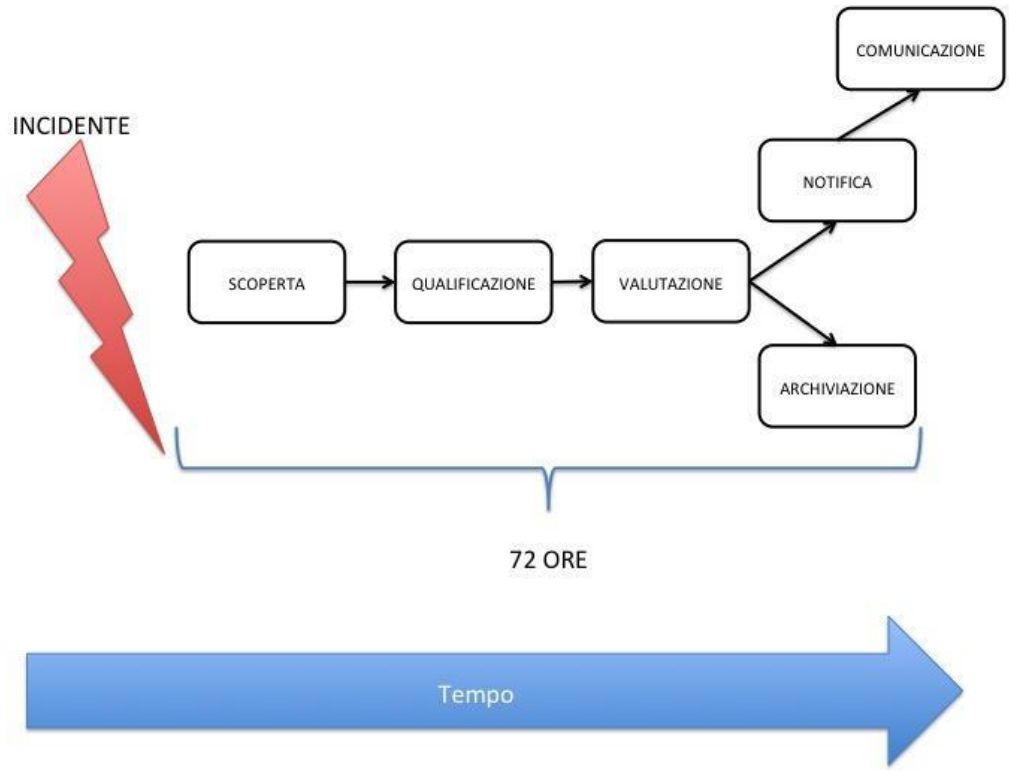
- internamente, attraverso le liste di distribuzione dei referenti di rete (refrete@units.it) e dei tecnici informatici (tecsia@units.it),
- internamente, attraverso le liste di distribuzione a tutto il personale di Ateneo e/o ad un sotto-insieme (es. Responsabili di Struttura, Personale Docente, ecc…),
- con il GARR-CERT - Computer Emergency Response Team della comunità dell'istruzione e della ricerca nazionale,
- con il CERT-PA - Computer Emergency Response Team Pubblica Amministrazione,
- con il CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.
- Con il Compartimento Polizia Postale e delle Comunicazioni per il Friuli V.G.

Per gli aspetti relativi alla protezione dei dati, in particolare il data breach, è attivo l'indirizzo mail dpo@units.it cui rivolgersi per contattare il RPD - Responsabile della Protezione dei Dati dell'Ateneo.

Il nominativo è pubblicato nel portale di Ateneo, in Amministrazione Trasparente.

Procedura in caso di data breach

I processi che descrivono la successione temporale di procedure e azioni in caso di data breach sono descritti nella seguente immagine, e devono svilupparsi nell'arco temporale massimo di 72 ore:



Nell'eventualità in cui si constati o si sospetti un evento di data breach (***scoperta***) è necessario inviare tempestivamente una notifica all'indirizzo sicurezzainformatica@units.it nel quale si indicano gli elementi utili ad avviare gli approfondimenti del caso (***qualificazione***): data dell'evento, ammontare e tipologia di dati coinvolti, categoria di interessati, modalità attraverso cui è avvenuto l'incidente e come è stato rilevato, ecc…

I soggetti autorizzati, al fine di segnalare l'evento all'indirizzo mail suindicato, devono utilizzare il modello proposto dal Garante per la protezione dei dati personali, limitatamente alle Sezioni A-B-C. Il modello è disponibile al seguente indirizzo:
https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=2.0. È consigliato anche un contatto diretto col team che presidia la Sicurezza Informatica di Ateneo mediante telefonata al numero 040 5583331.

Il team Sicurezza Informatica entro 12 ore informa il RPD (dpo@units.it) ed il gruppo di supporto al RPD, contatta i responsabili e/o le persone designate dell'Area dei Servizi ICT, dei Dipartimenti o altra struttura periferica nonché, se del caso, dell'Amministrazione Centrale per la gestione dell'incidente e la continuità operativa e, in caso di accertata gravità, preavvisa il Titolare.

Valutazione di pertinenza

Entro 12 ore dalla segnalazione il Team Sicurezza Informatica si riunisce con massima priorità, anche in remoto, con il RPD al fine di valutare la pertinenza dell'evento segnalato.

Durante il primo incontro il Team:

- ❏ Raccoglie le informazioni necessarie al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato;
- ❏ Individua eventuali soggetti autorizzati che devono essere coinvolti per la raccolta di ulteriori informazioni;
- ❏ Valuta prioritariamente eventuali azioni per contenere gli effetti dell'evento, comprese precise istruzioni da dare ai soggetti autorizzati coinvolti;
- ❏ Entro il termine della riunione o della call conference, il comitato di gestione della crisi definisce se l'evento segnalato integri una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche;
- ❏ Valuta il ruolo nel trattamento dei dati personali e, qualora l'Ateneo effettui il trattamento in qualità di Responsabile del trattamento ex art. 28 GDPR o di Contitolare ex art. 26 GDPR, comunica immediatamente l'evento al Titolare del trattamento;
- ❏ Redige il Verbale del primo incontro, recante la decisione assunta.

Valutazione del rischio, raccolta di informazioni e adozione di misure di mitigazione

Entro 24 ore dalla segnalazione il Team Sicurezza informatica effettua con l'assistenza dell'RPD l'analisi dei rischi per valutare, ai fini della eventuale segnalazione all'Autorità garante, le conseguenze della violazione dei dati personali per gli interessati coinvolti e la gravità della violazione, in particolare:

a) se sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche;
b) se sia necessario effettuare una comunicazione del data breach agli interessati coinvolti;

c) quali misure di mitigazione adottare per interrompere gli effetti del data breach o contenerne gli effetti.

Nel caso a) non è necessario procedere alla notifica all'Autorità garante o nei confronti degli interessati. L'incidente viene archiviato ma viene in tutti i casi inserito un record nel registro interno delle violazioni di Ateneo (Registro Data Breach) a cura del Team Sicurezza. Gli eventi di sicurezza che non comportano un trattamento di dati personali o i meri bug non devono essere riportati nel Registro.

L'analisi dei rischi è effettuata seguendo i criteri di cui alle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 WP250rev.01 - Gruppo di lavoro Articolo 29 per la protezione dei dati".

Nell'ambito delle attività e del termine suindicati, sotto il coordinamento del team Sicurezza Informatica, tutti i settori operativi coinvolti effettuano un'analisi relativa all'incidente e forniscono al RPD gli elementi utili a descriverlo ai fini della sua ***valutazione***. Le informazioni vengono raccolte, ad uso esclusivamente interno, compilando il modello di notifica predisposto dal Garante per la protezione dei dati personali, limitatamente alla Sezione D "Informazioni di dettaglio sulla violazione". In caso di necessità, provvedono alla continuità operativa dei servizi e al contenimento dell'incidente, ove ancora in corso, nonché ripristino della disponibilità dei dati. Rendicontano al RPD ogni azione intrapresa in tal senso.

In base ai dati raccolti, ove necessario, entro le successive 24 ore il Titolare ***notifica*** all'Autorità Garante l'incidente e lo comunica al Titolare.

La notifica deve perlomeno:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. comunicare il nome e i dati di contatto del RPD;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. 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.
5. deve essere utilizzato il modello predisposto dal Garante per la protezione dei dati personali pubblicato al seguente indirizzo, e già utilizzato nelle precedenti fasi interne per la raccolta di informazioni durante l'istruttoria:
   https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=2.0

In base alla valutazione del Titolare, sentito il RPD, 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. La comunicazione avviene ad opera dell'ufficio individuato in relazione all'interessato/i coinvolto/i e descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno i punti 2), 3) e 4) dell'elenco precedente.

Nell’eventualità in cui detta comunicazione richiederebbe sforzi sproporzionati, la violazione viene resa pubblica attraverso canali generici quali ad esempio un avviso sul portale web di Ateneo ovvero utilizzando i Social Media.

In base alla valutazione del RPD, non si procede con la comunicazione all'interessato se:

1. 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;
2. 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;
3. la comunicazione richiederebbe sforzi sproporzionati e si è adottato il metodo della comunicazione pubblica come precedentemente indicato.

In caso di eventi particolarmente gravi o complessi, la qualificazione e successiva analisi dell’evento stesso di data breach può richiedere un processo di approfondimento con tempistiche incompatibili rispetto ai termini di legge (72 ore dalla scoperta, Regolamento UE 2016/679, art. 33). In tal caso, il Titolare, se non è in grado di raccogliere tutte le informazioni richieste entro il termine, effettua comunque la prima notifica entro le 72 ore e effettua successivamente ulteriori notifiche integrative;

Azioni successive

Una volta effettuate le notifiche di Data Breach, il RPD mantiene attivo il canale di comunicazione con il Garante e il referente interno indicato dal Team Sicurezza mantiene attivo il canale di comunicazione con gli interessati destinatari della notifica, oltre a sovrintendere le ulteriori attività per mitigare i rischi residui, qualora le azioni già adottate non siano ritenute sufficienti per rimuovere le vulnerabilità riscontrate.