Linee guida per la gestione operativa dei *data breach*

Maggio 2019

Sommario

PREMESSA 3
Definizione di violazione dei dati personali (*data breach*) 3
Tipi di violazioni dei dati personali 4
Obblighi del responsabile del trattamento 5
La notifica al Garante per la protezione dei dati personali 5
La comunicazione agli interessati 6
1. IL PROCESSO DI GESTIONE DEL *DATA BREACH* SU ARCHIVI DIGITALI 7
1.1 Attori del processo 7
1.1.1 CERT del MIUR 7
1.1.2 Unità di presidio regionale 8
1.1.3 Altri attori coinvolti 8
1.2 Fasi del processo 8
1.2.1 Acquisizione del potenziale *data breach* 9
1.2.2 Asseverazione del *data breach* 9
1.2.3 Notifica e comunicazione del *data breach* 10
2.PROCESSO DI GESTIONE *DATA BREACH* RELATIVI AD ARCHIVI CARTACEI 11
2.1 Tipologie di violazione di dati 11
2.2 Il processo di *data breach* 11
2.2.1 Gli attori del processo 11
2.2.2 Le fasi del processo 12
2.2.3 Acquisizione del potenziale *data breach* 12
2.2.4 Asseverazione del *data breach* 12
2.2.5 Notifica e comunicazione del *data breach* 13
3.ALLEGATI 13
3.1 Allegato A: "modello di comunicazione incidente violazione dati personali" 13
3.2 Allegato B: "scheda di valutazione del *data breach*" 14
3.3 Allegato C: "Registro degli incidenti di sicurezza" 14
3.4 Allegato D:"Template notifica al Garante Privacy" 14
3.5 Allegato E "Template comunicazione all'interessato" 14
3.6 Allegato F: "Modello di comunicazione incidente violazione dati personali presenti su archivi cartacei" 14

PREMESSA

Il regolamento generale sulla protezione dei dati (in seguito "Regolamento") introduce l'obbligo di notificare una violazione dei dati personali all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Il Regolamento rende la notifica obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

Il Gruppo di lavoro ex articolo 29[1] ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi. All'atto della notifica all'autorità di controllo, il Titolare può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. L'autorità di controllo, infatti, può ordinare al Titolare di informare le persone fisiche interessate dalla violazione. La comunicazione dell'avvenuta violazione alle persone fisiche interessate consente al Titolare di fornire loro informazioni sui rischi derivanti e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione stessa. Allo stesso tempo, va evidenziato come la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo possa comportare l'irrogazione di una sanzione al Titolare ai sensi dell'articolo 83 del Regolamento.

Il Regolamento in linea generale prevede che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire una loro adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Pertanto, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

Definizione di violazione dei dati personali (*data breach*)

La violazione di dati personali è un particolare tipo di incidente di sicurezza.

Il dato personale oggetto della violazione può essere presente su archivi ed avere una rappresentazione sia digitale che cartacea[2].

Per porre rimedio a una violazione dei dati personali occorre innanzitutto che il Titolare sia in grado di riconoscerla. All'articolo 4, punto 12, il Regolamento definisce la "violazione dei dati personali" come "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".

1 Il cosiddetto Gruppo di lavoro ex articolo 29 è un organismo consultivo e indipendente, istituito dall'articolo 29 della Direttiva 95/46 del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il Gruppo di lavoro ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018 (entrata in vigore del Regolamento). Con il nuovo Regolamento europeo il Gruppo di lavoro è stato sostituito dall'organismo europeo "European Data Protection Board".

2 Per data breach su archivi digitali s'intende qualsiasi violazione di dato personale presente sui componenti del sistema informatico.Ad esempio, il data breach digitale può verificarsi su dati presenti su piattaforme, sistemi in cloud, su dispositivi e supporti digitali (es. USB key, CD, DVD, …), nonché sulle postazioni di lavoro fisse e mobili.

Il significato di "distruzione" dei dati personali è chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare. Anche il concetto di "danno" è evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si intende il caso in cui i dati esistono, ma il Titolare può averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a riceverli (o ad accedere a) oppure qualsiasi altra forma di trattamento in violazione del Regolamento.

Tipi di violazioni dei dati personali

Le violazioni di dati personali possono essere classificate in base a tre diverse tipologie connesse alla sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale di dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è semplice, 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.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del Regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità di dati personali per un certo periodo di tempo costituisce una violazione se la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12, del Regolamento.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5 del Regolamento. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere

o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il Titolare dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33 del Regolamento, il Titolare dovrà effettuare la notifica solo nel caso in cui la violazione dei dati personali comporta un probabile rischio per i diritti e le libertà delle persone fisiche. Questo aspetto dovrà essere valutato caso per caso.

Obblighi del responsabile del trattamento[3]

Sebbene il Titolare conservi la responsabilità generale per la protezione dei dati personali, il Responsabile del trattamento svolge un ruolo importante nel consentire al Titolare di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, del Regolamento dispone che il ruolo del Responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il Responsabile del trattamento "assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento".

L'articolo 33, paragrafo 2, del Regolamento chiarisce che, se il Titolare ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, il Responsabile del trattamento deve notificarla al Titolare "senza ingiustificato ritardo". Va evidenziato che il Responsabile del trattamento non deve valutare la probabilità di rischio sui diritti e le libertà delle persone fisiche derivante dalla violazione prima di notificarla al Titolare; spetta, infatti, a quest'ultimo effettuare tale valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e notificarla al Titolare.

La notifica al Garante per la protezione dei dati personali

La notifica ha la funzione di consentire all'autorità di controllo, ossia al Garante per la protezione dei dati personali, di applicare le misure correttive a sua disposizione (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ecc.) previste dall'articolo 58 del Regolamento e di adottare misure di tutela immediate a favore soggetti coinvolti. Elemento centrale della procedura di notificazione è la sua **tempestività**.

In generale, è necessario notificare **al Garante per la protezione dei dati personali, entro le 72 ore, l'avvenuto *data breach***. E' importante che sia dimostrabile il momento dell'asseverazione della violazione, poiché da quel momento decorrono le 72 ore per la notifica. Qualora la notifica al Garante per la protezione dei dati personali non sia effettuata entro 72 ore, dovrà essere corredata dei motivi del ritardo.

L'articolo 33 del Regolamento prescrive al soggetto che esercita le funzioni di Titolare (ossia, Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) di documentare qualsiasi violazione dei dati personali, al fine di consentire al Garante per la protezione dei dati personali di verificare il rispetto della norma. Pertanto, tutte le generali

3 Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.

attività di scoperta e di trattamento dell'incidente devono essere documentate, adeguate, tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Qualora il Titolare non sia in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva del *data breach*, il Regolamento (articolo 33, paragrafo 4) prevede che, le informazioni possano essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Gruppo di lavoro ex articolo 29 chiarisce come il Regolamento consente al Titolare di utilizzare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

- La prima tecnica è l'utilizzo dell'**"approssimazione"**. Il Titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.
- Secondo strumento previsto dal Regolamento è la **"notificazione in fasi"**. In questo caso il Titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie, ma dopo una prima e rapida notifica di allert, può adempiere agli obblighi di notifica comunicando tutte le informazioni per fasi successive, aggiornando di volta in volta lo stesso Garante sui nuovi riscontri.
- Il Regolamento prevede la possibilità di effettuare una "notifica differita" dopo le 72 ore previste dall'articolo 33 nel caso in cui, ad esempio, si subiscano violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio dilazionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Se il Titolare omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34 del Regolamento, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'irrogazione di una sanzione amministrativa pecuniaria appropriata in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, del Regolamento oppure come sanzione indipendente.

La comunicazione agli interessati

Accanto agli obblighi di notifica al Garante per la protezione dei dati personali, l'articolo 34 del Regolamento prevede in capo ai Titolari un **obbligo di comunicazione** agli interessati, che consenta loro di attivarsi a tutela dei propri interessi.

Come evidenziato dalle Linee guida del Gruppo di lavoro ex art. 29, i due obblighi sono innescati dal superamento di soglie di rischio differenti: è sufficiente un rischio "semplice" per far scattare l'obbligo di notifica, mentre è necessario un rischio "elevato" per attivare quello di comunicazione.

L'adeguatezza di una comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Le Linee guida del Gruppo di lavoro ex art. 29, sulla base dell'art. 34 del Regolamento, ricordano che devono sempre essere privilegiate modalità di

comunicazione dirette con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrebbe essere comunicato in maniera chiara e trasparente, evitando di inviare le informazioni che potrebbero essere facilmente fraintese dai destinatari. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es: l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Anche in questo caso, il Regolamento è attento a non gravare i Titolari di oneri eccessivi prevedendo che, nel caso in cui la segnalazione diretta richieda sforzi sproporzionati, questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea, però, che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti banner o notifiche disposte sul sito istituzionale, non lo sarà se questa sia limitata all'inserimento della notizia nella rassegna stampa.

La comunicazione, secondo quanto previsto dall'articolo 34 del Regolamento, deve contenere almeno le seguenti informazioni:

- la comunicazione del nome e dei dati di contatto del Responsabile della protezione dei dati previsto dall'articolo 37 del Regolamento o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e alla gestione dei possibili effetti negativi.

La comunicazione all'interessato non è richiesta se:

- il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. In tale circostanza, il Titolare deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

1. IL PROCESSO DI GESTIONE DEL *DATA BREACH* SU ARCHIVI DIGITALI

1.1 Attori del processo

1.1.1 CERT del MIUR

La responsabilità di gestire il processo generale degli **incidenti di sicurezza sui sistemi informativi del MIUR gestiti a livello centrale** è affidata al **CERT (Computer Emergency Response Team) del MIUR**.

Il CERT è una unità di presidio nominata con decreto del Direttore della Direzione generale per i contratti, gli acquisti e per i sistemi informativi e la statistica (di seguito DGCASIS) ed è costituita da referenti del MIUR che si occupano della sicurezza informatica.

Il CERT ricopre un ruolo fondamentale nel processo del *data breach*, in quanto:

- gestisce il processo degli incidenti di sicurezza;
- elabora rapporti sulla gestione degli incidenti di sicurezza;
- analizza la vulnerabilità sui sistemi, sulle applicazioni e sulle infrastrutture IT;
- rappresenta il contatto operativo con le autorità esterne al MIUR in tema di sicurezza informatica (es. CERT-PA, CNAIPIC) e con gli altri enti afferenti al mondo MIUR (es. Indire, Invalsi, Cineca, ecc.);
- supporta il Titolare nella notifica del *data breach* asseverato a livello centrale al Garante per la protezione dei dati personali.

1.1.2 Unità di presidio regionale

La responsabilità della gestione degli **incidenti di sicurezza verificatisi sui sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali** è affidata all'unità di presidio regionale. Ciascun Dirigente preposto all'Ufficio scolastico regionale nomina con decreto il Responsabile e i componenti dell'unità di presidio regionale. L'unità di presidio regionale, qualora lo ritenga opportuno, può essere coadiuvata dal CERT del MIUR nell'attività di analisi e gestione del *data breach.*

1.1.3 Altri attori coinvolti

- **Titolare** - il soggetto che esercita le funzioni di Titolare del trattamento (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione viene informato del sospetto *data breach*, notifica il *data breach* asseverato al Garante per la protezione dei dati personali e, ove necessario, comunica la violazione agli interessati senza ingiustificato ritardo;
- **Dirigente competente** – segnala il potenziale *data breach* e supporta il CERT o l'unità di presidio regionale, fornendo utili elementi di valutazione;
- **Ufficio di Gabinetto del Ministro** – è informato, nei casi in cui la violazione è di particolare rilevanza in relazione alle attività del Ministero, del *data breach* asseverato e avvia, ove ritenuto necessario, le opportune attività di comunicazione;
- **Responsabile della protezione dei dati** - è costantemente informato a partire dal sospetto di *data breach.*

1.2 Fasi del processo

Il processo prevede tre fasi:

- Acquisizione del potenziale *data breach*;
- Asseverazione del *data breach*;

- Notifica e comunicazione del *data breach*.

Figura 1 – Fasi del processo di *data breach*

1.2.1 Acquisizione del potenziale *data breach*

La fase di "Acquisizione" rappresenta il momento nel quale il MIUR viene a conoscenza del sospetto che un *set* di dati personali sono stati esfiltrati o compromessi.

Nel caso di **incidenti di sicurezza sui sistemi informativi del MIUR gestiti a livello centrale**, si provvede a segnalare immediatamente il sospetto di violazione dati personali al CERT.

Pertanto, i Dirigenti degli Uffici del MIUR, qualora rilevino, nel proprio contesto organizzativo, su segnalazione interna (dipendenti del proprio ufficio) o su segnalazione di terzi, la presenza di una possibile **violazione dei dati personali presenti sui sistemi informativi del MIUR gestiti a livello centrale,** ne danno immediata comunicazione al CERT, tramite la casella di posta elettronica dedicata: CERT@istruzione.it, compilando e inviando il modulo allegato (Allegato A: "modello di comunicazione incidente violazione dati personali"). Tale comunicazione va inoltrata per conoscenza alla propria figura di vertice della struttura di riferimento (Capo di Gabinetto, Capo Dipartimento, Direttore Generale), alla DGCASIS e al Responsabile della protezione dei dati.

Nel caso in cui l'incidente coinvolga dati personali presenti su **sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali** del MIUR la segnalazione dovrà essere effettuata dai dirigenti competenti all'unità di presidio regionale, dandone immediata comunicazione anche al Dirigente preposto all'Ufficio scolastico regionale e al Responsabile della protezione dei dati sulla base del modello di cui all' allegato A "modello di comunicazione incidente violazione dati personali". L'unità di presidio regionale valuterà l'opportunità di chiedere il supporto del CERT.

Le segnalazioni da parte dei Responsabili del trattamento, di CERT-PA, di CNAIPIC o di altri enti esterni dovranno essere immediatamente inoltrate dagli uffici competenti al CERT tramite la casella di posta elettronica dedicata: CERT@istruzione.it o all'unità di presidio regionale se non riguarda i sistemi informativi del MIUR gestiti a livello centrale.

1.2.2 Asseverazione del *data breach*

Nella fase di asseverazione del *data breach*, il CERT o l'unità di presidio regionale, in collaborazione con la struttura di riferimento che ha segnalato l'incidente, analizza il sospetto incidente al fine di asseverare l'esistenza del *data breach*.

In particolare, il CERT o l'unità di presidio regionale, supportati dal Dirigente del MIUR che ha segnalato l'incidente sia a livello centrale che periferico e dal relativo Referente privacy della struttura di riferimento, approfondiscono e analizzano la fattispecie nel rispetto dei termini previsti dall'articolo 33 del Regolamento, al fine di rilevare:

- la natura dell'eventuale violazione dei dati personali subita (tipologia di incidente, descrizione servizio impattato/banca dati/archivio fisico oggetto di *data breach*, intervallo temporale di riferimento, luogo dell'incidente, ecc.);
- il numero (anche approssimativo) e le categorie degli interessati e i dati personali oggetto di violazione;
- le possibili conseguenze della violazione sui diritti e sulle libertà dell'interessato e la valutazione della probabilità che le stesse si verifichino ai fini dell'eventuale notificazione al Garante per la protezione dei dati personali;
- le misure di sicurezza in essere e applicate ai dati violati;
- le eventuali misure adottate per porre rimedio alla violazione e/o per attenuarne gli effetti negativi.

Al termine dell'analisi, il CERT o l'unità di presidio regionale elabora una scheda di valutazione del *data breach* (Allegato B) in cui indica la causa, lo scenario di emersione, il potenziale impatto, le azioni già compiute e altre informazioni ritenute utili.

In caso di *data breach* asseverato su sistemi informativi del MIUR gestiti a livello centrale, il CERT trasmette la scheda di valutazione del *data breach* (Allegato B) al soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento) nella struttura i cui dati sono stati oggetto di violazione, nonché per conoscenza alla DGCASIS, alla Direzione generale competente e, per *data breach* di particolare rilevanza, al Capo di Gabinetto.

In caso di *data breach* asseverato su sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali del MIUR, l'unità di presidio regionale trasmette la scheda di valutazione del *data breach* (Allegato B) al Dirigente preposto all'Ufficio scolastico regionale e al CERT per le attività di competenza, nonché per conoscenza alla DGCASIS e, per *data breach* di particolare rilevanza, al Capo di Gabinetto. Anche in caso di falso positivo, l'unità di presidio regionale trasmette la scheda al CERT.

Il CERT, sia in caso di asseverazione del *data breach* sia in caso di falso positivo, aggiorna il Registro degli incidenti di sicurezza (Allegato C).

1.2.3 Notifica e comunicazione del *data breach*

Entro 72 ore dal momento in cui il CERT o l'unità di presidio regionale assevera la violazione, è necessario procedere alla **notifica del *data breach*** secondo quanto previsto dall'articolo 33 del Regolamento**.**

In caso di violazione asseverata su sistemi informativi del MIUR gestiti a livello centrale, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento) nella struttura i cui dati sono stati oggetto di violazione, supportato dalla DGCASIS, notifica il *data breach* al Garante per la protezione dei dati personali, utilizzando il *template* fornito dallo stesso Garante (Allegato D).

In caso di violazione asseverata su sistemi informativi gestiti in via autonoma dagli Uffici Scolastici Regionali, il Dirigente preposto all'Ufficio scolastico regionale notifica il *data breach* al Garante per la protezione dei dati personali utilizzando il *template* fornito dallo stesso Garante (Allegato D).

Il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione, ove necessario (cfr. par. La comunicazione agli interessati), **comunica la violazione** agli interessati senza ingiustificato ritardo utilizzando il modello "Template comunicazione all'interessato" (Allegato E) secondo quanto previsto dall'articolo 34 del Regolamento.

In relazione alla rilevanza del *data breach* possono essere coinvolti, ove necessario:

- **Ufficio di Gabinetto:** pianifica la comunicazione esterna al MIUR coinvolgendo l'Ufficio stampa;
- **CERT:** informa CNAIPIC e CERT-PA;
- **DGCASIS:** pianifica la comunicazione interna al MIUR tramite l'ufficio competente.

2.PROCESSO DI GESTIONE *DATA BREACH* RELATIVI AD ARCHIVI CARTACEI

2.1 Tipologie di violazione di dati

La violazione di dati presenti in via esclusiva su archivi cartacei può aver luogo sia per eventi accidentali che per eventi dolosi.

Tra gli eventi accidentali rientrano gli eventi anomali avvenuti per:

- distruzione accidentale di documenti (incendio o allagamento dei locali dove sono presenti archivi cartacei);
- distruzione per errore di documenti originali, senza avere il possesso di una eventuale copia;
- smarrimento di documenti;
- fornitura involontaria di dati a persona diversa dal destinatario.

Gli eventi dolosi possono avvenire per comportamenti posti in essere dal personale interno o da soggetti esterni realizzati attraverso:

- distruzione dei documenti;
- accesso non autorizzato;
- furto.

2.2 Il processo di *data breach*

2.2.1 Gli attori del processo

- **Titolare** - il soggetto che esercita le funzioni di Titolare del trattamento (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione viene informato del sospetto *data breach*, notifica il *data breach* asseverato a livello centrale o regionale al Garante per la protezione dei dati personali e, ove necessario, comunica la violazione agli interessati senza ingiustificato ritardo;
- **Dirigente competente** – segnala il potenziale *data breach*;
- **Ufficio di Gabinetto del Ministro** – è informato, nei casi in cui la violazione è di particolare rilevanza in relazione alle attività del Ministero, del *data breach* asseverato e avvia, ove ritenuto necessario, le opportune attività di comunicazione;

- **Responsabile della protezione dei dati** - è costantemente informato a partire dal sospetto di *data breach*;
- **CERT –** aggiorna, sia in caso di *data breach* asseverato che di falso positivo, il Registro degli incidenti di sicurezza (Allegato C).

2.2.2 Le fasi del processo

Il processo prevede tre fasi:

- Acquisizione del potenziale *data breach*;
- Asseverazione del *data breach*;
- Notifica e Comunicazione del *data breach*.

Figura 2 – Fasi del processo di *data breach* su archivi cartacei

2.2.3 Acquisizione del potenziale *data breach*

Il dirigente che viene a conoscenza dell'evento anomalo di violazione di dati personali deve comunicarlo, senza ingiustificato ritardo, con posta elettronica indicando come oggetto **"URGENTE: Potenziale *data breach* su archivi cartacei"**, alla propria figura di vertice della struttura i cui dati sono stati oggetto di violazione (Capo di Gabinetto, Capo Dipartimento, Direttore generale o Dirigente preposto all'Ufficio scolastico regionale) e, per conoscenza, al Responsabile della protezione dei dati, inviando il modulo "Modello di comunicazione incidente violazione dati personali presenti su archivi cartacei" (Allegato F).

2.2.4 Asseverazione del *data breach*

Il soggetto che ha ricevuto la segnalazione del potenziale *data breach*, coaudivato dal dirigente competente, approfondisce e analizza la fattispecie nel rispetto dei termini previsti dall'articolo 33 del Regolamento, al fine di rilevare:

- la natura dell'eventuale violazione dei dati personali subita (tipologia di incidente, descrizione servizio impattato/banca dati/archivio fisico oggetto di *data breach*, intervallo temporale di riferimento, luogo dell'incidente, ecc.);
- il numero (anche approssimativo) e le categorie degli interessati e i dati personali oggetto di violazione;
- le possibili conseguenze della violazione sui diritti e sulle libertà dell'interessato e la valutazione della probabilità che le stesse si verifichino ai fini dell'eventuale notificazione al Garante per la protezione dei dati personali;
- le misure di sicurezza in essere e applicate ai dati violati;
- le eventuali misure adottate per porre rimedio alla violazione e/o per attenuarne gli effetti negativi.

Al termine dell'analisi, il soggetto che ha ricevuto la segnalazione del potenziale *data breach* elabora una scheda di valutazione del *data breach* (Allegato B) in cui indica la causa, lo scenario di emersione, il potenziale impatto, le azioni già compiute e altre informazioni ritenute utili e dichiara l'asseverazione o meno del *data breach*.

In caso di *data breach* asseverato, il soggetto che ha ricevuto la segnalazione del potenziale *data breach* trasmette la scheda di valutazione del data breach (Allegato B) al soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) e, per *data breach* di particolare rilevanza, informa per conoscenza il Capo di Gabinetto.

Sia in caso di *data breach* asseverato che di falso positivo, è necessario trasmettere la scheda di valutazione del *data breach* (Allegato B) al CERT per l'aggiornamento del Registro degli incidenti di sicurezza (Allegato C).

2.2.5 Notifica e comunicazione del *data breach*

Entro 72 ore dal momento in cui il *data breach* è stato asseverato, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) procede alla **notifica del *data breach*** secondo quanto previsto dall'articolo 33 del Regolamento utilizzando il *template* fornito dallo stesso Garante (Allegato D).

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) della struttura i cui dati sono stati oggetto di violazione, **comunica la violazione** agli interessati senza ingiustificato ritardo utilizzando il modello "Template comunicazione all'interessato" (Allegato E) secondo quanto previsto dall'articolo 34 del Regolamento.

In relazione alla rilevanza del *data breach* possono essere coinvolti, ove necessario:

- **Ufficio di Gabinetto:** pianifica la comunicazione esterna al MIUR coinvolgendo l'Ufficio stampa;
- **DGCASIS:** pianifica la comunicazione interna al MIUR tramite l'ufficio competente.

3.ALLEGATI

3.1 Allegato A: "modello di comunicazione incidente violazione dati personali"

Allegato A Modello di comunicazione incider

3.2 Allegato B: "scheda di valutazione del *data breach*"

Allegato B Scheda di valutazione del data b

3.3 Allegato C: "Registro degli incidenti di sicurezza"

Allegato C - Registro degli incidenti di sicure

3.4 Allegato D:"Template notifica al Garante Privacy"

Allegato D Template notifica al Garante Pri

3.5 Allegato E "Template comunicazione all'interessato"

Allegato E Template comunicazione all'inte

3.6 Allegato F: "Modello di comunicazione incidente violazione dati personali presenti su archivi cartacei"

Allegato F Modello di comunicazione incider