INAF

ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

MANUALE PER LA GESTIONE DI DATA BREACH

secondo il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)

Introduzione

Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - RGDP) 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 (c.d. "*data breach*").

Il presente documento costituisce una Guida a beneficio dei dipendenti dell'Istituto Nazionale di Astrofisica incaricati dello svolgimento delle attività di trattamento dei dati e dei Responsabili delle attività di trattamento dei dati svolte per conto dell'Istituto, in qualità di titolare del trattamento.

Nella redazione del presente Manuale si è tenuto conto delle indicazioni e delle disposizioni:

- del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - RGDP);
- del Decreto legislativo 30 giugno 2003, numero 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto legislativo 10 agosto 2018, numero 101;
- del Gruppo "Articolo 29" all'interno delle Linee-guida in materia di notifica delle violazioni di dati personali, approvate, in via definitiva, il 6 febbraio 2018;
- del Garante per la protezione dei dati personali nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali".

Il presente Manuale è soggetto a integrazioni e modifiche alla luce dell'evoluzione normativa italiana, della riflessione che si svilupperà a livello nazionale ed europeo, nonché delle prassi che saranno, di volta in volta, riscontrate all'interno dell'Istituto.

1. Premessa: cosa si intende per "dato personale"?

Il Regolamento (UE) 2016/679 definisce il "dato personale" come "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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Dalla lettura della norma "dato personale" e "informazione" sembrerebbero coincidere; in realtà si tratta di concetti tra loro differenti. Più precisamente, si può affermare che il dato è la fonte dell'informazione, nel quale questa è contenuta e dal singolo dato o dall'insieme dei dati l'informazione può essere estratta o ricavata. Ma l'informazione, a rigore, non coincide con il dato: l'informazione è elaborazione del dato.

L'avvento della società digitale ha determinato un ampliamento notevole delle tipologie di dati che possono essere oggetto di trattamento; si pensi, ad esempio, alla videosorveglianza, che comporta il trattamento delle immagini, ai sistemi biometrici, che consentono di verificare l'identità di una persona mediante l'analisi dell'impronta digitale oppure attraverso la scansione dell'iride. Il concetto di "dato personale" appare oggi sempre più dilatato, fino a ricomprendervi qualunque contenuto informativo, dalla classica espressione alfabetica sino all'immagine o al suono: in tal senso, un "dato personale" non è necessariamente un dato testuale, ma anche un'immagine, una registrazione della voce, di una videoripresa. Ne discende che anche un suono o un fotogramma sono informazioni comprese nella definizione di "dato personale"; inoltre, soddisfano la definizione anche l'informazione irrilevante, quella positiva, l'informazione minima o la metainformazione, ossia l'informazione sull'informazione, non rilevando, ai fini della nozione di "dato personale", nemmeno la verità o la falsità del l'informazione: del resto, un'informazione falsa o imprecisa produce tendenzialmente effetti pregiudizievoli ancor più che un'informazione corretta. Si può pertanto affermare che, per precisa scelta del legislatore europeo, la nozione di "dato personale" è particolarmente ampia, anche sul piano applicativo, e non è un concetto facilmente limitabile.

Il nome, il cognome, la data di nascita sono tutti "dati" che consentono l'identificazione diretta dell'interessato e sono riconducibili alla nozione di dati identificativi, ossia dati che non comportano particolari operazioni di ricostruzione per identificare in maniera diretta l'interessato. Ma anche un indirizzo IP si configura come dato personale: in un recente caso del 2016 (CGE, 19 ottobre 2016, C-482/2014, *Breyer*), la Corte di Giustizia Europea ha dichiarato che "un indirizzo di protocollo IP dinamico registrato da un fornitore di servizi di media on line in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale (…) nel caso in cui detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone".

Allo stesso modo, è opportuno sottolineare che la definizione di dato personale non fa riferimento, né direttamente né indirettamente, alla riservatezza: il dato personale non è necessariamente un dato riservato. Sono dati personali, ad esempio, il numero di matricola, il numero di telefono, l'indirizzo di posta elettronica: il dato personale può anche essere un dato conosciuto dai più.

2. Che cos'è una violazione dei dati personali?

Per poter porre rimedio a una violazione occorre innanzitutto essere 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".

In tal senso, si ha:

- "distruzione" dei dati, ogni qual volta gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento;
- "danno" quando i dati personali sono stati modificati, corrotti o non sono più completi;

- “perdita” dei dati personali nel caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l’accesso, oppure non averli più in possesso. Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento; oppure il caso in cui l’unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso;
- “trattamento non autorizzato o illecito” quando viene effettuata una divulgazione di dati personali a (o l’accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure quando viene svolta qualsiasi altra forma di trattamento in violazione del regolamento.

E’ chiaro, comunque, che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all’articolo 4, punto 12, il regolamento si applica soltanto in caso di violazione di *dati personali*. La conseguenza di tale violazione è che il titolare del trattamento non è più in grado di garantire l’osservanza dei principi relativi al trattamento dei dati personali di cui all’articolo 5 del Regolamento. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

3. Tipologia di violazioni dei dati personali

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro articolo 29 ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della 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 dei dati personali;

- "violazione della disponibilità", in caso di perdita, accesso[1] 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 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. Esempi di perdita di disponibilità possono aversi 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. 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.

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 dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.

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. Ciò aiuta il

[1] L'"accesso" è una componente fondamentale della "disponibilità". In tal senso, si veda il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", nonché la norma ISO/IEC 27000:2016, che definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato.

titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. 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 del trattamento 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, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato 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.

4. La notifica di una violazione di dati personali: la comunicazione all'Autorità di controllo ai sensi dell'articolo 33 del RGPD

Il Regolamento UE 2016/679 afferma[2] che una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in

[2] Regolamento (UE) 679/2016, Considerando 85

cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro articolo 29 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. Il titolare del trattamento è quindi 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.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione: in alcuni casi sarà relativamente evidente, fin dall'inizio, che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

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.

Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Inoltre, è espressamente previsto un onere informativo anche in capo al Responsabile del trattamento: questi, infatti, è tenuto ad informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

L'articolo 33 del Regolamento specifica altresì il "contenuto minimo" della notifica del Titolare del trattamento all'Autorità di controllo competente; la predetta notifica deve:

a) 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;
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 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 possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il paragrafo 5 dell'articolo 35 del RGPD impone altresì al titolare del trattamento di documentare qualsiasi violazione dei dati personali, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, al fine di consentire all'Autorità di controllo di verificare il rispetto della disposizione in esame.

Il Gruppo di lavoro articolo 29 ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi: all'atto della notifica all'autorità di controllo, infatti, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti

che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione. Qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno strumento per migliorare la conformità in materia di protezione dei dati personali. Allo stesso tempo, va osservato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al titolare del trattamento ai sensi dell'articolo 83.

La notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto che "*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*".

Ciò significa che il Regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1.

Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche

siano corrette. Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte. In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Circostanze nelle quali non è richiesta una notifica

L'articolo 33, paragrafo 1, chiarisce che se è "*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" tale violazione non è soggetta a notifica all'autorità di controllo. Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica.

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che una violazione della riservatezza di dati personali crittografati con un algoritmo all'avanguardia costituisce in ogni caso una violazione dei dati personali e deve essere notificata. Se però la riservatezza della chiave rimane intatta (ossia se la chiave non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in maniera tale da non poter

essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi), in linea di principio i dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata. Tuttavia, anche se i dati sono crittografati, una perdita o alterazione può avere effetti negativi per gli interessati ove il responsabile del trattamento non disponga delle necessarie copie di riserva. In tal caso, la notifica agli interessati dovrebbe essere necessaria anche se sono state adottate misure di protezione mediante crittografia.

Viceversa, se i dati personali sono stati resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un *backup*, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo, poiché è improbabile che tale violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Di conseguenza, potrebbe non essere necessario nemmeno informare la persona interessata, dato che è improbabile che vi siano rischi elevati. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione può cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Ad esempio, se la chiave risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel software di cifratura, è possibile che sia ancora necessario procedere alla notifica.

Inoltre, va osservato che se si verifica una violazione in assenza di *backup* dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di *backup* dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per ripristinare i dati dal *backup* e dell'effetto che la mancanza di disponibilità ha sulle persone fisiche. Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*".

Esempio

Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Tuttavia, si avrà mancato rispetto dell'articolo 33 se il titolare del trattamento non effettua la notifica all'autorità di controllo nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la qualità e la corretta attuazione della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è appropriato in ragione dei rischi presentati. Il titolare del trattamento dovrebbe altresì avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura. Ad esempio, un dispositivo può essere crittografato una volta spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare obsoleta nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

5. La notifica di una violazione di dati personali: la comunicazione agli interessati ai sensi dell'articolo 34 del RGPD

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate. L'articolo 34, paragrafo 1, afferma che "*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".

Il titolare del trattamento dovrebbe 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[3]. 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.

L'articolo 34, paragrafo 2, del Regolamento precisa che "*La comunicazione all'interessato (…) descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)*"; in sostanza, il titolare del trattamento deve fornire, secondo tale disposizione, almeno 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.

[3] Regolamento (UE) 679/2016, Considerando 86

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato; in tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c). 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. 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. Inoltre, il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi di comunicazioni con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il considerando 86 spiega che "*Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*". Il titolare del trattamento

potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "*conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.

Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

Circostanze nelle quali non è richiesta una notifica

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche;
- 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.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[4]. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

6. Gestione di un *data breach*: procedura e misure specifiche

Il presente documento ha lo scopo di indicare alle Strutture di ricerca dell'Istituto Nazionale di Astrofisica le opportune modalità di gestione di un *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016, e della disciplina interna dettata dal Consiglio di Amministrazione dell'Ente per la definizione della organizzazione delle attività di trattamento (Delibera del 20 novembre 2018, numero 106).

In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione di un *data breach*, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare per il tramite del referente privacy (Fase 1);
- analisi delle segnalazioni e valutazione dell'evento accaduto (Fase 2);
- modalità e profili di segnalazione all'Autorità Garante e agli interessati (Fase 3);
- registrazione e segnalazione nel registro dei *data breach* (Fase 4);
- analisi post violazione (Fase 5).

[4] Cfr. articolo 5, paragrafo 2, del RGPD.

È necessario che ogni Struttura di ricerca dia notizia a tutti i dipendenti in merito alla presente procedura mediante idonea circolare. In conformità alla delibera del Consiglio di Amministrazione del 20 novembre 2018, numero 106, ogni Direttore di Struttura è individuato quale "Referente privacy" ed è affiancato da un "Gruppo privacy" (o "Data Protection Local Unit" - "DPLU"), gruppo multidisciplinare di dipendenti che supportano il referente privacy per specificità tecniche quali ICT, area giuridica, area del personale, etc., che, ai fini della presente procedura, riveste il ruolo di Data Breach Assessment Unit ("**DBAU**").

Il referente privacy assume, ai fini della presente procedura, il ruolo di responsabile del processo.

Fase 1: raccolta delle informazioni

A: Canali Interni

Le segnalazioni interne di eventi anomali possono:

- pervenire dal personale dell'Istituto;
- essere inoltrate dal Responsabile della Protezione dei Dati.

B: Canali Esterni

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili esterni delle attività di trattamento.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'Istituto la verifica dell'eventuale violazione.

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al Responsabile della Protezione dei Dati comunque non oltre 12 ore dalla conoscenza della violazione, all'indirizzo rpd@inaf.it o, ove possibile e preferibilmente, a mezzo PEC all'indirizzo rpd-inaf@legalmail.it.

La presa in carico di tutte le segnalazioni è di responsabilità della DBAU che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

Fase 2: analisi delle segnalazioni e valutazione dell'evento

A: Analisi preliminare della segnalazione e compilazione della scheda evento

La DBAU avvia un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento (Allegato A), contenente tutte le informazioni raccolte:

- data evento anomalo;
- data presunta di avvenuta violazione;
- data e ora in cui si è avuto conoscenza della violazione;
- fonte segnalazione;
- tipologia violazione e di informazioni coinvolte;
- descrizione evento anomalo;
- numero Interessati coinvolti;
- numerosità di Dati Personali di cui si presume una violazione;
- indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di *device* mobili;
- sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene quindi destinata alla valutazione di primo livello descritta di seguito.

B: Valutazione di primo livello - Verifica della segnalazione

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non sia un cd. "falso positivo". Nel caso la violazione su dati personali venga accertata, la DBAU, responsabile dell'analisi di primo livello, con la collaborazione degli Uffici/Servizi coinvolti dalla violazione, recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento. Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente; l'evento viene comunque inserito a cura della DBAU nel Registro dei Data Breach (Allegato C), tenuto dal RPD, nella apposita sezione dedicata agli "eventi falsi positivi".

C: Valutazione di secondo livello - Scheda violazione dati

Per l'analisi di secondo livello viene convocata dal Direttore Generale la "Data Protection Management Unit" ("**DPMU**") che, ai sensi della delibera del Consiglio di Amministrazione del

20 novembre 2018, numero 106, è un gruppo permanente a cui partecipano stabilmente

- il Responsabile dell'Ufficio "ICT Management e Science Data Management" della Struttura Tecnica della Direzione Scientifica;
- il Responsabile dell'articolazione organizzativa "Servizi Informatici e per il Digitale" della Direzione Generale;
- il Responsabile della Protezione dei Dati;
- il Responsabile del Servizio di Staff "Affari Legali, Contenzioso e Supporto Tecnico agli Organi".

Per la corretta e tempestiva gestione delle emergenze, la composizione della "Data Protection Management Unit" (che, ai fini della presente procedura, riveste il ruolo di "Data Breach Management Unit" - "**DBMU**") può essere integrata, su disposizione del Direttore Generale, a seconda della entità e delle caratteristiche del *Data Breach* subìto.

In tutti i casi, il DBMU analizza congiuntamente tutte le informazioni raccolte e redige una Scheda Violazione Dati (Allegato B) per le conseguenti valutazioni.

Il DBMU classifica l'evento tra i seguenti casi:

- distruzione di dati illecita;
- perdita di dati illecita;
- modifica di dati illecita;
- distruzione di dati accidentale;
- perdita di dati accidentale;
- modifica di dati accidentale;
- divulgazione non autorizzata;
- accesso ai dati personali illecito.

La violazione deve essere valutata secondo i livelli di rischio:

- **NULLO**
- **BASSO**
- **MEDIO**
- **ALTO**

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

1. discriminazioni;
2. furto o usurpazione d'identità;
3. perdite finanziarie;
4. pregiudizio alla reputazione;
5. perdita di riservatezza dei dati personali protetti da segreto professionale;
6. decifratura non autorizzata della pseudonimizzazione;
7. danno economico o sociale significativo;
8. privazione o limitazione di diritti o libertà;
9. impedito controllo sui dati personali all'interessato;
10. danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti 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 a condanne penali e a reati o alle relative misure di sicurezza;
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 di persone fisiche vulnerabili, in particolare minori;
d) che il trattamento riguardi una notevole quantità di Dati Personali;
e) che il trattamento riguardi un vasto numero di Interessati.

Il DBMU deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

Fase 3: notifica e comunicazione

A: Notifica all'Autorità Garante

Redatta la Scheda Violazione Dati, il DBMU deve valutare le azioni da intraprendere ed avviare la notificazione verso l'Autorità di controllo e, ove necessario, la comunicazione agli interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

Il RPD notifica la violazione all'Autorità di controllo competente 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 e dunque sia stato dallo stesso classificato "**NULLO**".

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, va corredata dei motivi del ritardo. La notifica all'Autorità di controllo deve:

a) descrivere, ove possibile:
   i. la natura della violazione dei dati personali;
   ii. le categorie e il numero approssimativo di Interessati;
   iii. le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del RPD 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 dell'Istituto 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 possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

B: Comunicazione della violazione all'interessato

Il Responsabile della Protezione dei Dati, sentito il Direttore Generale, deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli articoli 33 e 34 del

Regolamento, il DBMU valuti che la violazione risulta presentare rischi classificati come "***ALTI***" nella Scheda Violazione Dati (Allegato B) per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo; deve essere effettuata ad opera del DBMU e deve essere intellegibile, concisa, trasparente, e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato. Rispetto alle modalità della comunicazione si applicano quelle ritenute più idonee dal DBMU.

La comunicazione di Data Breach all'interessato deve contenere le seguenti informazioni:

a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
b) natura della violazione dei dati personali;
c) nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
d) le probabili conseguenze della violazione dei dati personali;
e) una descrizione sintetica delle misure adottate o di cui si propone l'adozione da parte dell'Istituto per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) sono state messe 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 incomprensibili a chiunque non sia autorizzato ad accedervi (sono fatti salvi i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati);
b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche (in tal caso è necessario documentare le misure nella scheda di violazione);
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.

In allegato alla presente Guida (Allegato D) è disponibile un Fac-simile di comunicazione all'interessato della violazione dei dati personali.

Fase 4: registrazione e segnalazione nel registro dei *data breach*

Nel Registro dei Data Breach (Allegato C)**,** la DBAU documenta ogni singolo evento, sia esso, "***Falso***", "***Irrilevante***" ovvero "***Rilevante***"; in quest'ultimi due casi, devono essere indicate nel registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notificazione all'Autorità di Controllo;
- l'eventuale comunicazione all'interessato.

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle violazioni di dati personali.
Il Registro dei Data Breach è tenuto a cura del Responsabile della Protezione dei Dati sotto la responsabilità dell'Istituto Nazionale di Astrofisica, titolare del trattamento.

Fase 5: analisi post violazione

L'ultima fase del processo di gestione delle violazioni di dati personali prevede 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.
Tale attività prevede il coinvolgimento della Sezione "***ICT Management e Science Data Management***" ("***ICT***") della Direzione Scientifica e dell'articolazione organizzativa "***Servizi Informatici e per il Digitale***" ("***SID***") della Direzione Generale, con eventuale supporto da parte di altri Uffici/Servizi.

7. *Data breach* presso un Responsabile esterno del trattamento

Quando un terzo agisce in qualità di Responsabile esterno della attività di trattamento svolte per conto e nell'interesse dell'INAF, in caso di violazione dei dati personali, deve informare l'Istituto (che agisce in qualità di Titolare), senza ingiustificato ritardo e non al più tardi di 24 ore dal momento in cui ha conoscenza della violazione, inviando una comunicazione ai seguenti indirizzi [ove possibile via PEC]:

- rpd@inaf.it
- rpd-inaf@legalmail.it [PEC]

e successivamente collaborare con l'Istituto per consentirgli di adempiere agli obblighi previsti dalla normativa agli articoli 33 e 34 del Regolamento. La procedura che segue è riportata come allegato nel Contratto per il Trattamento dei Dati Personali, salvo diversamente concordata con il Responsabile.

[quanto segue è consigliabile ma ci si aspetta che responsabili strutturati abbiano già procedure interne che rifletteranno gli obblighi di legge, e che quindi in pratica la procedura si concluderà qui. Ove invece il responsabile sia destrutturato e non abbia procedure per il caso di data breach, si consiglia di proseguire come segue]

Il Responsabile deve assistere l'Istituto avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento utilizzando il modello allegato alla presente Guida, contenente tutte le informazioni raccolte:

- data evento, anche la data presunta di avvenuta violazione (in tal caso va specificato);
- data e ora in cui si è avuto conoscenza della violazione;
- fonte della segnalazione;
- tipologia di violazione e di informazioni coinvolte;
- descrizione evento anomalo;
- numero di interessati coinvolti;
- numerosità di dati personali di cui si presume una violazione;
- indicazione della data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza;

- indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di *device* mobili;
- sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Una volta condotta l'analisi preliminare, il Responsabile esterno deve condurre un'analisi di primo livello per verificare che la segnalazione non tratti un falso positivo; all'esito dell'accertamento, qualora si tratti di un falso positivo il Responsabile esterno deve comunicarlo immediatamente all'INAF agli stessi indirizzi di cui sopra, al fine di consentirgli di inserire l'evento nella sezione "eventi falsi positivi" del Registro dei Data Breach (Allegato C).

In caso contrario, il Responsabile recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento che deve essere inviata, possibilmente via PEC, tempestivamente e non oltre 24 ore dalla conoscenza della violazione, al Responsabile della Protezione dei Dati dell'INAF.

L'evento deve essere inserito dall'Istituto in un apposito Registro dei Data Breach, il cui modello è allegato alla presente Guida, e, una volta ricevuta la Scheda Evento, l'INAF deve procedere secondo le prescrizioni di cui alla lettera C della "Fase 2", alla "Fase 3", alla "Fase 4" e alla "Fase 5" di cui al Paragrafo 6 della presente Guida.

Allegato A - Scheda evento

SCHEDA EVENTO	
Codice	
Data evento e ora della violazione anche solo presunta (specificando se è presunta)	
Data e ora in cui si è avuta conoscenza della violazione	
Fonte della segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero di interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

Allegato B - Scheda violazione dati

SCHEDA VIOLAZIONE DATI		
Codice evento[1]	**Classificazione**[2]	**Rischio**[3]

1. Inserire il codice della scheda evento

2. La Data Breach Assessment Unit (DBAU) classifica l'evento tra i seguenti casi:
   - distruzione di dati illecita;
   - perdita di dati illecita;
   - modifica di dati illecita;
   - distruzione di dati accidentale;
   - perdita di dati accidentale;
   - modifica di dati accidentale;
   - divulgazione non autorizzata;
   - accesso ai dati personali illecito.

3. La Data Breach Management Unit (DBMU) valuta il rischio secondo i seguenti livelli:
   - **NULLO**
   - **BASSO**
   - **MEDIO**
   - **ALTO**

Allegato C - Registro dei *data breach*

Evento				Conseguenze	Provvedimenti adottati	Notifica all'Autorità di controllo		Comunicazione all'interessato	
Codice[4]	Irrilevante	Falso positivo	Rilevante			SI/NO	Data	SI/NO	Data

4. Inserire il codice della scheda evento

Allegato D - Modello di comunicazione all'interessato della violazione dei dati personali

Secondo quanto prescritto dall'articolo 34 del Regolamento Generale in materia di protezione dei dati personali (Regolamento (UE) 679/2016), l'Istituto Nazionale di Astrofisica, titolare del trattamento, con la presente è a comunicarLe l'intervenuta violazione dei Suoi dati personali (*data breach*), che si è verificata in data[5] _____, alle ore[6] _____ (e/o, di cui si è avuta conoscenza in data _____ alle ore_____).

A) Descrizione della natura della violazione:

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

b) Tipo di violazione, per esempio:
- ❖ Lettura (presumibilmente i dati non sono stati copiati)
- ❖ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ❖ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ❖ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ❖ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione

c) Dispositivo oggetto di violazione
- ❖ Computer
- ❖ Rete
- ❖ Dispositivo mobile
- ❖ Strumento di backup
- ❖ Documento cartaceo

d) Tipo di dati oggetto di violazione, per esempio:
- ❖ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ❖ Dati di accesso e di identificazione (username, password, altro)
- ❖ Dati personali idonei a rivelare l'origine razziale ed etnica
- ❖ Dati personali idonei a rivelare le convinzioni religiose
- ❖ Dati personali idonei a rivelare le convinzioni filosofiche o di altro genere
- ❖ Dati personali idonei a rivelare le opinioni politiche
- ❖ Dati personali idonei a rivelare l'adesione a partiti politici o a sindacati
- ❖ Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico, religioso, politico, sindacale
- ❖ Dati personali idonei a rivelare lo stato di salute
- ❖ Dati personali idonei a rivelare la vita sessuale
- ❖ Dati giudiziari
- ❖ Dati genetici
- ❖ Dati biometrici
- ❖ Ancora sconosciuti

B) Descrizione delle probabili conseguenze della violazione di dati personali[7]:

_____

_____

_____

C) Descrizione delle misure tecnologiche e organizzative assunte per porre rimedio alla violazione e se del caso per contenere la violazione dei dati o per attenuarne i possibili effetti negativi: _____

_____

_____

_____

Per poter ottenere maggiori informazioni relativamente alla violazione in oggetto, può contattare il Responsabile della Protezione dei Dati dell'Istituto Nazionale di Astrofisica ai seguenti indirizzi:

Email: rpd@inaf.it
PEC: rpd-inaf@legalmail.it
Indirizzo: Viale del Parco Mellini, 84 - 00136 Roma
Numero telefonico dedicato: (+39) 06/35533255

Roma, ……..

Il Responsabile della Protezione dei Dati dell'Istituto Nazionale di Astrofisica

_____

_____

5. Indicare la data, se nota, altrimenti indicare la data in cui si viene a conoscenza della violazione.
6. Indicare l'ora, se nota, altrimenti indicare l'orario in cui si viene a conoscenza della violazione.
7. Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali: 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, danno economico o sociale significativo, privazione o limitazione di diritti o libertà, impedito controllo sui dati personali all'interessato, danni fisici, materiali o immateriali alle persone fisiche.