IL TRATTAMENTO DEI DATI PERSONALI.

DAI PRINCIPI GENERALI ALLE ISTRUZIONI OPERATIVE

Eleonora Bovo - Pisa 18.10.2018

Il GDPR ed i principi per il trattamento dei dati personali

- Liceità correttezza e trasparenza
- Limitazione delle finalità del trattamento
- Minimizzazione
- Esattezza e aggiornamento
- Limitazione della conservazione
- Integrità, riservatezza, sicurezza

Il fondamento della liceità nel trattamento

1. Obblighi di legge cui è soggetto il Titolare
2. Interesse pubblico o esercizio di pubblici poteri
3. Interesse legittimo prevalente del Titolare o di terzi
4. Adempimento di obblighi contrattuali
5. Interessi vitali della persona interessata o di terzi
6. Consenso

La concretizzazione dei principi

NORME PER IL TRATTAMENTO DEI DATI PERSONALI NELL'INFN

Istruzioni per il trattamento

Dai principi alle istruzioni

liceità

- Accertarsi che la raccolta dei dati sia giustificata da una effettiva base giuridica o comunque sia necessaria per eseguire compiti di interesse pubblico o connesso all'esercizio di poteri pubblici di cui è titolare l'INFN

liceità

- Nel caso in cui il dato che si intende raccogliere non sia giustificato da una diversa base giuridica o non sia strettamente necessario per il raggiungimento dei compiti di interesse pubblico, far sottoscrivere all'interessato una dichiarazione di consenso

Il consenso

Deve essere libero, specifico, informato, inequivocabile ed "esplicito"

Non è ammesso il consenso tacito o presunto

(no a caselle pre-spuntate su un modulo).

Dai principi alle istruzioni

Limitazione della finalità del trattamento.

- Nella modulistica per la raccolta dei dati personali acquisire soltanto i dati necessari e pertinenti alla finalità per i quali sono raccolti

Esattezza ed aggiornamento

- Verificare l'esattezza dei dati raccolti, nonché la correttezza della loro scritturazione o digitazione

Dai principi alle istruzioni

Minimizzazione

- Utilizzare i dati personali in base al principio del “need to know”

Riservatezza

- Non trasmettere all’esterno o a terzi dati personali conosciuti in ragione della propria attività, salvo che si tratti di comunicazioni funzionali all’attività lavorativa

Dai principi alle istruzioni

Integrità e riservatezza

- Conservare la riservatezza dei dati personali conosciuti nello svolgimento dell'attività lavorativa anche dopo il trasferimento ad altra attività ed anche successivamente alla cessazione del rapporto di lavoro

Integrità e riservatezza

- Adottare tutte le misure necessarie a non rendere conoscibili neppure accidentalmente i dati personali a soggetti non autorizzati

Dai principi alle istruzioni

Correttezza e trasparenza

- Fornire agli interessati l'informativa sul trattamento in tutte le circostanze in cui si raccolgono dati personali

RACCOLTA DATI = INFORMATIVA

Contenuto dell'informativa

- i dati di contatto del Titolare e del DPO
- le finalità del trattamento e la base giuridica
- i legittimi interessi perseguiti dal Titolare
- gli eventuali destinatari dei dati
- l'eventuale trasferimento dei dati in un paese terzo o una organizzazione internazionale

Contenuto dell'informativa

- la natura obbligatoria o facoltativa del conferimento dei dati
- il periodo di conservazione dei dati
- la garanzia del diritto di rettifica, cancellazione o limitazione del trattamento
- il diritto di proporre reclamo al Garante per la tutela dei dati personali

Indicazioni ulteriori a seconda delle modalità di trattamento

- Trattamento con strumenti elettronici

- Trattamento senza strumenti elettronici

Istruzioni per il trattamento con strumenti elettronici

- Sicurezza fisica
- Antivirus
- Fishing
- Backup
- Corretta individuazione ed uso delle password
- Corretto uso della posta elettronica

Istruzioni per il trattamento senza strumenti elettronici

- Diligenza nella gestione dei documenti in lavorazione
- Conservazione dei documenti in archivi ad accesso controllato
- Corretto uso delle stampanti o fax condivisi
- Cautela nell'uso della carta riciclata
- Usare apparecchi distruggi documenti o modalità analoghe per disfarsi di documentazione contenente dati personali

Data Breach

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

Quanti Data Breach?

- Working Party art. 29 ha individuato tre categorie di violazioni:
  - *Confidentiality breach*: divulgazione o accesso ai dati personali accidentale o non autorizzata
  - *Integrity breach*: alterazione accidentale o non autorizzata di dati personali
  - *Availability breach*: perdita di accesso o distruzione di dati accidentale o non autorizzata

Cosa fare in caso di Data Breach

Notificare la violazione al **Garante** a meno che risulti improbabile che la violazione dei dati personali presenti **un rischio per i diritti e le libertà delle persone fisiche**

Comunicare la violazione **all'interessato** nel caso in cui la violazione presenti un **rischio elevato per i diritti e le libertà delle persone fisiche**

I tempi di azione

- La notifica al Garante deve essere effettuata **senza ritardo o comunque entro 72 ore** dal momento in cui si è avuta conoscenza della violazione

- Anche la comunicazione all'interessato deve essere fatta **senza ritardo**

Quando si ha conoscenza della violazione?

- Dipende dal caso concreto, ma in caso di potenziale violazione è necessario accertare quanto più velocemente possibile e con un ragionevole grado di certezza, se c'è stata la violazione.

Un fac simile per la notificazione

INFN Istituto Nazionale di Fisica Nucleare

Luogo, data .....

All'Autorità Garante per la protezione dei dati personali
PEC: protocollo@pec.gpdp.it

NOTIFICA DI VIOLAZIONE DI DATI PERSONALI
Art. 33 Regolamento UE in materia di protezione dei dati personali

Il sottoscritto …… Nato a …….. il ……. cod. fisc. …… in qualità di Direttore di (Laboratorio/Sezione/Centro) dell'Istituto Nazionale di Fisica Nucleare – INFN con sede in …… via …… n. …… cap. …… provincia ……., cod. fisc. …….. in ragione dei compiti assegnati ex art 2 quaterdecies del D.Lgs. n. 196/2003 e s.m.i. con deliberazione del Consiglio Direttivo INFN n. 14844 del 27.7.2018,

NOTIFICA

l'avvenuta violazione di dati personali i cui tempi e modalità sono descritti di seguito nel dettaglio.

DATA e ORA in cui si è verificata la violazione dei dati personali: ……..

DATA e ORA in cui il Responsabile del trattamento è venuto a conoscenza della violazione ……
Attenzione: ove la notifica non sia effettuata nelle 72 ore da quando il Responsabile ne sia venuto a conoscenza è necessario precisare i motivi che non hanno consentito la notificazione entro il termine temporale indicato dal Regolamento UE
……..
……..

NATURA DELLA VIOLAZIONE DEI DATI PERSONALI ……..
……..
……..

CATEGORIE DEI DATI PERSONALI INTERESSATI ALLA VIOLAZIONE ……..
……..
……..

NUMERO (anche approssimativo) DEGLI INTERESSATI I CUI DATI SONO STATI VIOLATI ……
……..

NUMERO DI REGISTRAZIONI DEI DATI PERSONALI VIOLATI ……
……..
……..

PROBABILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI PERSONALI ……..
……..

MISURE ADOTTATE O CHE CI SI PROPONE DI ADOTTARE PER RIMEDIARE ALLA VIOLAZIONE O PER ATTENUARNE GLI EFFETTI NEGATIVI ……..
……..
……..

D.P.O. INFN (nominativo e dati di contatto) ……..
……..
Il sottoscritto dichiara che tutta la documentazione afferente la violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio sono disponibili presso …… e resta altresì a disposizione per fornire ogni eventuale ulteriore informazione richiesta.

Il Direttore

Istituto Nazionale di Fisica Nucleare
codice fiscale 84001850589
Presidenza INFN - Piazza dei Caprettari 70 - 00186 Roma (Italia) - https://www.presid.infn.it
tel. +39 06 6840031 - fax +39 06 68307924 - email: presidenza@presid.infn.it - segreteria@presid.infn.it - prot@presid.infn.it - PEC: presidenza@pec.infn.it

Il contenuto della notificazione

- a) natura della violazione dei dati personali compresi le categorie e il numero approssimativo di interessati coinvolti;
- b) nome e i dati di contatto del Titolare e del DPO o di altro punto di contatto presso cui ottenere ulteriori informazioni;
- c) probabili conseguenze della violazione dei dati personali;
- d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali ed attenuarne i possibili effetti negativi

Notificare anche in assenza di notizie dettagliate sulla violazione

- L'assenza di informazioni precise circa la violazione rilevata, non costituisce ostacolo per una notificazione tempestiva: il GDPR richiede una prima notificazione per approssimazione circa il numero di persone coinvolte, le categorie di interessati e tipologie di dati violati, consentendo di fornire ulteriori dettagli in seguito, mediante una **notificazione per fasi**

Notificazione per fasi

- Nel caso in cui ci siano violazioni per incidenti di sicurezza complessi, entro le 72 è necessario procedere alla notificazione al Garante con i dati disponibili e dar seguito quindi alle ulteriori indagini per acquisire altri dettagli da notificare successivamente, comunque senza ingiustificato ritardo.

- Nella notifica per fasi è necessario informare il Garante che le informazioni trasmesse non sono complete e che ci saranno fasi successive di notificazione.

Notificazione tardiva

- E’ tardiva la notificazione effettuata oltre le 72 ore
- Il GDPR la consente
- E’ necessario indicare le ragioni del ritardo

Comunicazione agli interessati

In caso di rischio elevato per i diritti e le libertà delle persone

- comunicazione

Rischio elevato

- Quando la violazione può arrecare danni fisici, materiali o immateriali per coloro i cui dati sono stati violati:
  - Danni alla salute
  - discriminazione
  - furto d'identità
  - frode
  - perdite finanziarie
  - danno alla reputazione

La valutazione del rischio

- Per la valutazione di probabilità e gravità del rischio occorre tenere in considerazione:
  - Il tipo di violazione
  - La natura, sensibilità e volume dei dati personali
  - L'agevole identificazione degli interessati
  - La gravità delle conseguenze
  - Le specifiche caratteristiche degli interessati
  - Le specifiche caratteristiche dei Titolari
  - Il numero di interessati coinvolti

Cosa comunicare agli interessati

- la natura della violazione
- il nome ed i dati di contatto del DPO o altro punto di contatto
- le probabili conseguenze della violazione
- le misure adottate o che si intendono adottare per affrontare la violazione, incluse le misure per mitigare i possibili effetti negativi

Come contattare gli interessati

In modo diretto

Con messaggi dedicati alla sola comunicazione della violazione

Ipotesi in cui la comunicazione agli interessati non è dovuta

quando immediatamente dopo la violazione sono state adottate misure che scongiurino il concretizzarsi di un alto rischio per i diritti e le libertà delle persone

quando immediatamente dopo la violazione sono state adottate misure che scongiurino il concretizzarsi di un alto rischio per i diritti e le libertà delle persone

quando contattare i singoli comporta uno sforzo sproporzionato; in questi casi è possibile fare una comunicazione pubblica o adottare altre misure simili attraverso le quali gli interessati possano ugualmente avere effettiva notizia della violazione

Il Registro delle violazioni

- Necessario per documentare ogni violazione di dati personali.
- Deve essere reso disponibile al Garante ove questi lo richieda.

Il Registro delle violazioni: contenuto

- circostanze che caratterizzano le violazioni
- conseguenze
- I provvedimenti adottati per porvi rimedio
- Ogni decisione adottata in occasione della rilevata violazione

Grazie!