Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Dai principi alle indicazioni operative: La designazione del Responsabile del trattamento

Eleonora Bovo – Roma 12 aprile 2019

Titolare e Responsabile

Definizioni art. 4. Reg. UE 2016/679

Titolare del trattamento:

L'autorità pubblica (tra le altre) che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento** di dati personali

Responsabile del trattamento:

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del Titolare** del trattamento

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il Responsabile del trattamento

In tutte le circostanze in cui l'INFN affida ad un soggetto esterno lo svolgimento di un **servizio che coinvolga il trattamento di dati personali**, deve designare tale soggetto come **Responsabile del trattamento**.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il Responsabile del trattamento

Art. 28 Regolamento UE 2016/679

"Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato."

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il Responsabile del trattamento

E’ tenuto a strutturare il trattamento dei dati personali in modo da rappresentare al Titolare (ove richiesto anche al Garante) le garanzie necessarie a soddisfare le prescrizioni del Regolamento e la tutela dei diritti degli interessati

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Organizzazione del trattamento

Il Registro delle attività di trattamento

Deve consentire

- La dimostrazione della conformità del trattamento al Regolamento europeo
- La cooperazione con il Garante Privacy
- Il monitoraggio del Garante Privacy

Il Registro delle attività di trattamento

Deve essere

- Tenuto in forma scritta, anche in formato elettronico
- Aggiornato al variare di qualunque elemento che ne costituisce il contenuto

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il Registro delle attività di trattamento

Contiene:

- **Il nome e i dati di contatto del responsabile del trattamento, di ogni titolare del trattamento per conto del quale agisce e, ove applicabile, del responsabile della protezione dei dati**
- **Le categorie di trattamenti effettuati per conto di ogni titolare**
- **I trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione e, per i trasferimenti a soggetti che ne siano legittimati, la documentazione di garanzie adeguate**
- **La descrizione delle misure di sicurezza tecniche e organizzative previste dall'art. 32 del Regolamento**

Analisi dei rischi

E’ propedeutica alla valutazione delle misure da adottare; consente di gestire il rischio relativo al trattamento e di individuare le misure di sicurezza adeguate al trattamento effettuato in concreto.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

I canoni per la protezione dei dati

Privacy by design

- **Adozione di misure tecniche ed organizzative adeguate, dirette ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati**

Privacy by default

- **Adozione di misure adeguate a garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento.**

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Privacy by default

Adozione di misure adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento

Vale per:

La quantità dei dati raccolti;

La portata del trattamento;

Il periodo di conservazione;

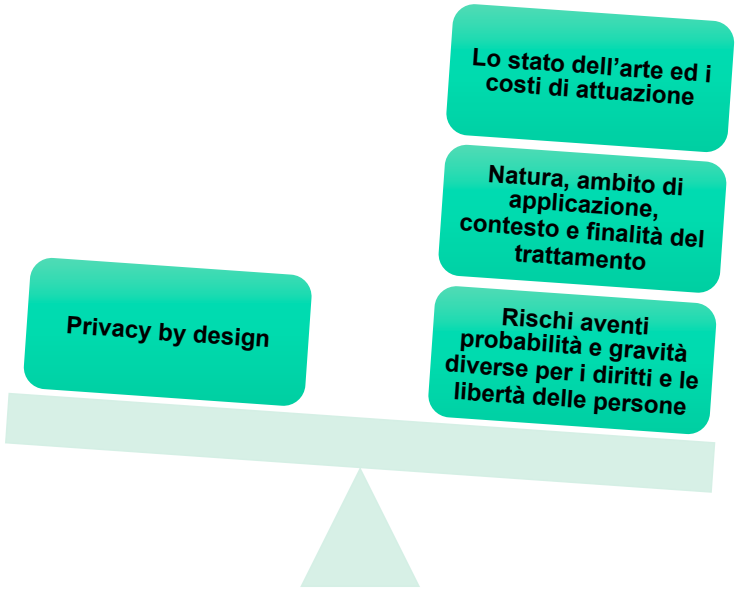
L'accessibilità

Per impostazione predefinita non possono essere resi accessibili dati personali a un numero indefinito di persone senza l'intervento di una persona fisica

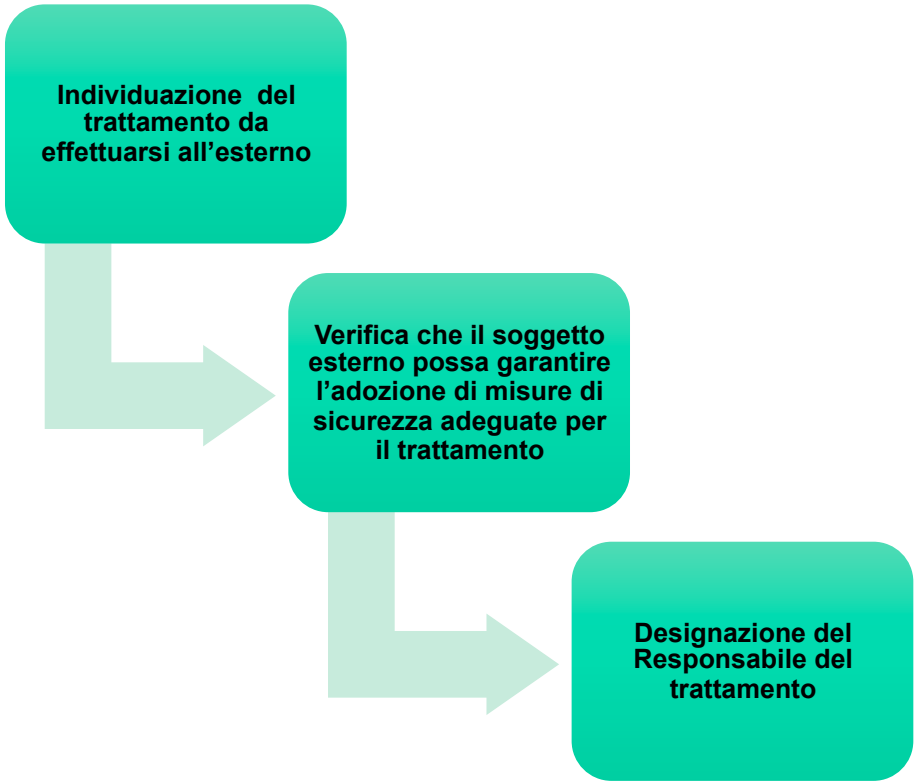
Privacy by design

Sia al momento di determinare i mezzi del trattamento

Sia all'atto del trattamento



La designazione del Responsabile del trattamento



La designazione del Responsabile del trattamento

L'art. 28 Reg. UE 2016/679 richiede un **contratto** o altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento e che individui la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto per la designazione del responsabile del trattamento

1. in esso si manifesta l'accordo delle parti per regolare un rapporto giuridico
2. contiene la disciplina del rapporto
3. è fonte di obbligazioni

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il contenuto del contratto

- Impegno ad effettuare il trattamento secondo le istruzioni documentate del Titolare
- Impegno alla riservatezza delle persone autorizzate al trattamento dei dati personali o indicazione che dette persone siano tenute ad un adeguato obbligo legale di riservatezza
- Impegno all'adozione di adeguate misure di sicurezza
- Divieto di ricorrere ad altro Responsabile salva previa autorizzazione scritta del Titolare

Il contenuto del contratto

- impegno del Responsabile ad assistere il Titolare, con misure adeguate, per dar seguito alle richieste per l'esercizio dei diritti degli interessati
- impegno del Responsabile ad assistere il Titolare in tutte le attività connesse alla valutazioni del rischio inerente i dati, alla loro sicurezza e alla eventuale violazione
- impegno del Responsabile a cancellare o restituire i dati al termine del rapporto che ne giustifica il trattamento
- impegno del Responsabile a rendere disponibili al Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dalla legge e dal Regolamento UE.

Lo schema di contratto nell'INFN

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI

CONTRATTO PER LA DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI.

28 FEBBRAIO 2019

L'ISTITUTO NAZIONALE DI FISICA NUCLEARE (di seguito anche INFN) con sede legale in via E. Fermi, 40 Frascati (Roma), Codice Fiscale: 84001850589, in persona del Presidente pro-tempore/del Direttore ..... della Struttura INFN di .....]

TITOLARE DEL TRATTAMENTO

e

L'operatore economico/ altro soggetto ..... con sede ..... Codice Fiscale: ....., in persona del legale rappresentante/persona appositamente autorizzata giusta delega .....

RESPONSABILE DEL TRATTAMENTO

congiuntamente definite anche Parti,

premesso che

- il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito anche Regolamento) dispone che il soggetto che effettui un trattamento dei dati personali per conto del Titolare è individuato Responsabile del trattamento e vincolato a una condotta conforme ai principi indicati nel Regolamento nonché all'adozione di misure tecniche e organizzative adeguate per una efficace protezione dei dati personali;

Lo schema di contratto nell'INFN

le Parti in epigrafe individuate e rappresentate

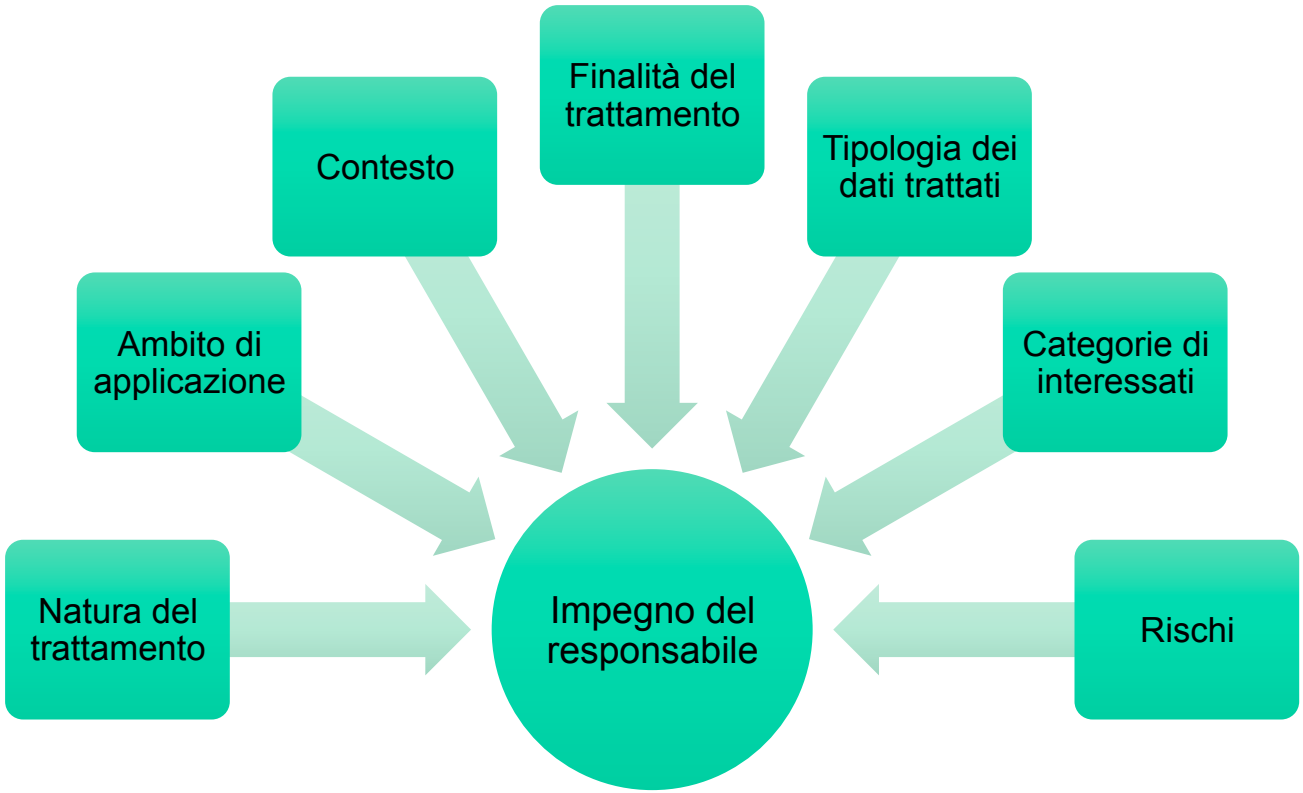
convengono e stipulano quanto segue.

Le premesse formano parte integrante e sostanziale del presente contratto.

L'INFN individua l'operatore economico/altro soggetto …….. Responsabile del trattamento dei dati personali trattati per suo conto

Per la durata del contratto… il Responsabile del trattamento dei dati personali designato, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia di dati personali trattati, delle categorie di interessati nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, si impegna nei confronti del Titolare a:

L'impegno del responsabile del trattamento



Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

L'impegno all'osservanza dei principi stabiliti dal Reg. UE 2016/679

Il Responsabile del trattamento dei dati personali designato …. si impegna a:

a. trattare i dati personali nel rispetto dei princìpi e delle disposizioni previsti dal Codice, dal Regolamento, dagli indirizzi e dai provvedimenti a carattere generale emanati dal Garante in materia di protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

I principi per il trattamento dei dati personali

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

Il fondamento della liceità

Il trattamento è lecito se:

1. l'interessato ha espresso il consenso
2. è necessario all'esecuzione di un contratto
3. è necessario per adempiere ad un obbligo legale
4. è necessario per la salvaguardia di un interesse vitale
5. è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
6. è necessario al perseguimento di un legittimo interesse

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il fondamento della liceità

Decreto Legislativo 17 marzo 1995, n. 230,

in particolare capo VIII “Protezione sanitaria dei lavoratori”

Decreto Legislativo 9 aprile 2008, n. 81

In materia di tutela della salute e della sicurezza nei luoghi di lavoro

Trasparenza e correttezza

L'informativa sul trattamento:

- chiara, semplice, trasparente,
- intellegibile, facilmente accessibile
- forma scritta, anche in formato elettronico

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

L'informativa dell'INFN

Disponibile all'indirizzo web:
https://dpo.infn.it/

NOTA INFORMATIVA DI CARATTERE GENERALE SUL TRATTAMENTO DEI DATI PERSONALI NELL'INFN

4 Dicembre 2018

La presente informativa viene resa ai sensi del Regolamento UE 2016/679, Regolamento Generale per la Protezione dei Dati (nel seguito Regolamento) e del D.Lgs. 30 giugno 2003 n. 196 ess.mm.ii., Codice in materia di protezione dei dati personali, al fine di informare le persone fisiche che forniscono i propri dati personali all'Istituto Nazionale di Fisica Nucleare (INFN nel seguito) su come questi sono raccolti, utilizzati, consultati o altrimenti trattati, nonché la misura in cui sono o saranno trattati .

TITOLARE DEL TRATTAMENTO

Istituto Nazionale di Fisica Nucleare, con sede in Frascati, via E. Fermi 40.

email presidenza@presid.infn.it
PEC amm.ne.centrale@pec.infn.it)

RESPONSABILE DELLA PROTEZIONE DEI DATI

L'INFN ha designato il Responsabile per la Protezione dei Dati (RPD o DPO) con deliberazione del Consiglio Direttivo n. 14734 del 27 aprile 2018.

Il DPO è contattabile presso l'indirizzo e-mail: dpo@infn.it

NATURA DEI DATI TRATTATI E FINALITÀ DEL TRATTAMENTO

I dati raccolti sono trattati dall'INFN per provvedere alla gestione dei rapporti di lavoro subordinato, di collaborazione o di formazione e di adempiere agli obblighi retributivi, previdenziali, fiscali, di tutela di salute e sicurezza nei luoghi di lavoro, di radioprotezione ed assicurativi previsti dalla legge, dai regolamenti e dalla contrattazione collettiva.

Categorie particolari di dati personali, quali quelli che rivelino l'origine razziale o etnica, l'appartenenza sindacale, le opinioni politiche, i dati relativi alla salute o all'orientamento sessuale, sono trattati esclusivamente nel limite necessario ad adempiere gli obblighi del titolare del trattamento in materia di:

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Dai principi alle indicazioni operative

Limitazione della finalità del trattamento.	• Acquisire soltanto i dati necessari e pertinenti alla finalità per le quali sono raccolti
Esattezza ed aggiornamento	• Verificare l'esattezza dei dati raccolti, nonché la correttezza della loro scritturazione o digitazione
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
Integrità e riservatezza	• Adottare tutte le misure necessarie a non rendere conoscibili neppure accidentalmente i dati personali a soggetti non autorizzati
Limitazione della conservazione	• Conservare i dati soltanto per il tempo previsto dal decreto legislativo n. 230/1995

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

L'osservanza delle Norme per il trattamento dei dati personali

Il Responsabile del trattamento dei dati personali designato …. si impegna a:

f. osservare quale livello minimo di sicurezza, le prescrizioni previste dal Contratto e dagli eventuali suoi allegati, adottando misure non inferiori alle *"Norme per il trattamento dei dati personali nell'INFN"* disponibili all'indirizzo web https://dpo.infn.it/ oltre, ove applicabili, le *"Linee guida per lo sviluppo del software sicuro"* pubblicate dall'Agenzia per l'Italia Digitale e ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati da parte del Responsabile;

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Indicazioni per il trattamento

- Adottare particolare cura e diligenza nella gestione dei documenti in lavorazione
- Conservare i documenti in archivi ad accesso controllato
- Evitare per il trattamento di dati di radioprotezione l'uso di stampanti o fax condivisi
- Fare attenzione all'uso di carta riciclata
- Utilizzare apparecchi distruggi documenti o modalità analoghe per disfarsi di documentazione contenente dati personali

Divieto di ricorrere ad altro responsabile

Il responsabile

- non ricorre a un altro Responsabile senza la previa autorizzazione scritta del Titolare;

- accerta che il l'ulteriore Responsabile offra garanzie sufficienti per l'adozione delle misure tecniche ed organizzative di sicurezza;

- impone all'ulteriore Responsabile i medesimi obblighi contenuti nella presente designazione;

- conserva, nei confronti del Titolare anche in caso di inadempimento dell'altro responsabile, l'intera responsabilità dell'adempimento di tali obblighi

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il trasferimento dei dati in Paesi terzi o organizzazioni internazionali

Il Responsabile del trattamento dei dati personali designato …. si impegna a:

d. non trasferire, né in tutto né in parte, in un Paese terzo o a un'organizzazione internazionale i dati personali trattati ai sensi del Contratto, senza la previa autorizzazione del Titolare

e. attenersi alle istruzioni fornite dal Titolare stesso, anche in caso di eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o la normativa nazionale; in tal caso, il Responsabile del trattamento informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il trasferimento dei dati in Paesi terzi o organizzazioni internazionali

Il trasferimento di dati è consentito se: (artt. da 45 a 49 Reg. UE 2016/679)

- Il Paese terzo o l'organizzazione internazionale garantiscono un livello di protezione adeguato secondo una valutazione effettuata dalla Commissione UE ("decisioni di adeguatezza")

- in mancanza di "decisioni di adeguatezza" consentito se il Titolare fornisce garanzie adeguate a che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi

- in ogni caso ove si verifichino circostanze che giustificano una deroga, tra cui:
  a. l'interessato abbia acconsentito al trasferimento
  b. il trasferimento sia necessario all'esecuzione di un contratto
  c il trasferimento sia necessario per tutelare interessi vitali dell'interessato

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il trasferimento dei dati in Paesi terzi o organizzazioni internazionali

Art. 65, 66, 68bis D.Lgs. n. 230/1995

Il datore di lavoro è tenuto ad assicurare la tutela dei lavoratori dai rischi di radiazioni ionizzanti in conformità alle norme del decreto stesso e in relazione all'entità complessiva del rischio anche nel caso in cui i lavoratori prestino la propria opera in impianti o laboratori/sedi gestiti da terzi

Nel caso di lavoratori i quali svolgono per più datori di lavoro attività che li espongono a rischi di radiazioni ionizzanti, ciascun datore di lavoro è tenuto a richiedere agli altri datori di lavoro ed ai lavoratori, e a fornire quando richiesto, le informazioni necessarie al fine di garantire il rispetto delle norme del presente capo e, in particolare, dei limiti di dose.

Su motivata richiesta di autorità competenti anche di altri paesi appartenenti all'Unione europea o di soggetti, anche di detti paesi, che siano titolari di incarichi di sorveglianza fisica o medica della radioprotezione del lavoratore, il lavoratore trasmette alle autorità o ai soggetti predetti le informazioni relative alle dosi ricevute.

Adozione ed implementazione delle misure di sicurezza

Il Responsabile del trattamento dei dati personali designato …. si impegna a:

j. **adottare tutte le misure di sicurezza** di cui all'art. 32 del Regolamento; nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, necessiti di una **valutazione d'impatto sulla protezione dei dat**i e/o evidenzi la necessità di approntare ulteriori misure di sicurezza, il Titolare può chiedere al Responsabile la loro **implementazione**; il Responsabile, nei casi in cui evidenzi una non piena corrispondenza tra la tipologia di trattamento prevista dal contratto/dalla convenzione e le misure di sicurezza richieste, si impegna a comunicarlo per scritto al Titolare, fornendogli l'analisi del rischio effettuata e indicando le misure di sicurezza che ritiene adeguate;

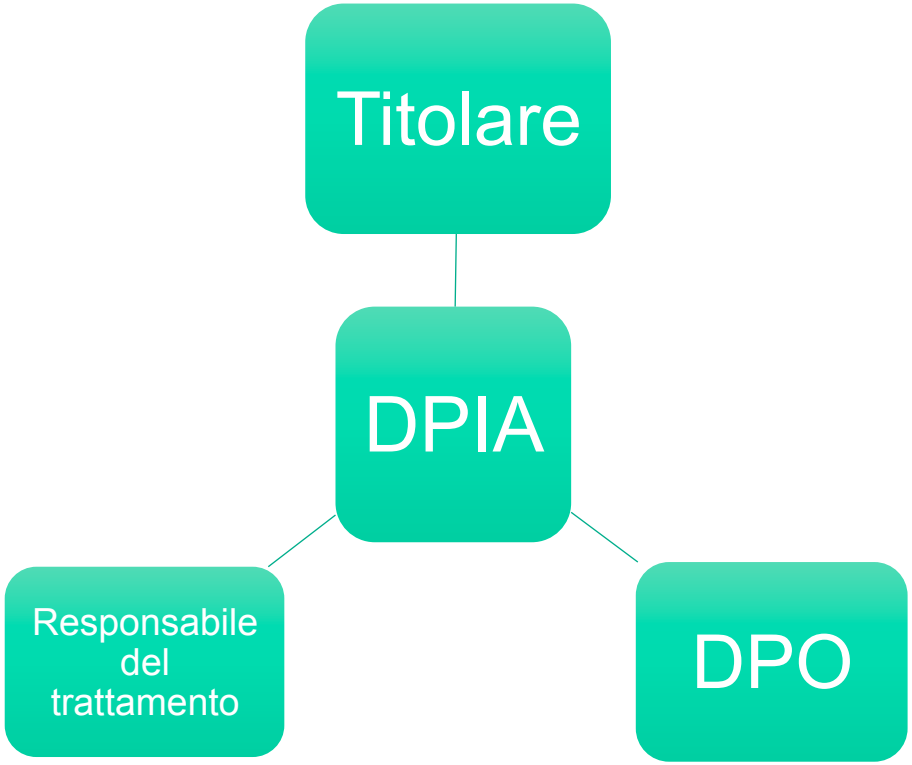
Misure di sicurezza e valutazione del rischio

Valutazione d'Impatto sulla Protezione dei Dati o Data Protection Impact Assessment (D.P.I.A.)

Strumento di valutazione del rischio necessario per i trattamenti che presentano rischi elevati (tra questi sono comprese le categorie particolari di dati personali)

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

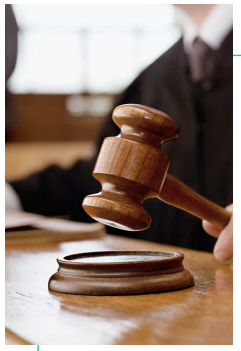
DPIA: i soggetti coinvolti



Il Procedimento di DPIA

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

L'assistenza al Titolare del trattamento



Nell'adempimento degli obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di accesso, rettifica, cancellazione, limitazione od opposizione al trattamento

Nel garantire il rispetto degli obblighi di sicurezza: oltre DPIA, comunicazione di ogni elemento che possa compromettere il corretto trattamento dei dati, nonché comunicazione di eventuali violazioni di dati (Data Breach)

Il Data Breach

Violazione di sicurezza nel trattamento di dati personali:

- ***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

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Adempimenti in caso di Data Breach

NOTIFICAZIONE della 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**

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

La notifica al Garante

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

La conoscenza della violazione:

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

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Il contenuto della notifica al Garante

a) Natura della violazione dei dati personali, compresi le categorie e il numero approssimativo di interessati coinvolti;

b) Nome e 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

Comunicazione agli interessati

Soltanto in caso di **rischio elevato** per i diritti e le libertà delle persone

Rischio elevato: se può arrecare danni fisici, materiali o immateriali tra cui:

- danni alla salute
- discriminazione
- furto d'identità
- danno alla reputazione

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Comunicazione delle violazioni per inserimento nel Registro

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

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Conseguenze per la violazione degli obblighi assunti

Art. 28, c. 10 Reg. UE 2016/679

Il responsabile che violi il Regolamento, determinando le finalità e i mezzi del trattamento è considerato Titolare del trattamento

Grazie!