T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# T4Data – Il progetto

**Luigi MONTUORI**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Il progetto T4Data

Progetto finanziato da Ue (REC) per la formazione di Autorità di controllo e RPD operanti nel settore pubblico

Obiettivi:
1) Rafforzamento conoscenze autorità di protezione dati
2) Supporto concreto a RPD settore pubblico

GDPR
GENERAL
DATA PROTECTION
REGULATION

# T4Data: «Deliverables»

I FASE: 2018
Formazione **Autorità di controllo**
Workshops, Seminari, **Manuale RPD**

II FASE: 2019
Formazione **RPD**
**Webinar ad-hoc**, **Seminari locali**

*Final Conference* (Roma)

III FASE: Post-2019
Diffusione contenuti a livello nazionale
Iniziative di sensibilizzazione

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# T4Data: I seminari locali di formazione

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

| Ancona | **Catanzaro** | Torino | Roma |
|---|---|---|---|
| 7 giugno | 26 giugno | 1 ottobre | 8 novembre |
| Sanità e ricerca | Trasparenza, accesso, *big data* | Sicurezza e gestione del rischio | Responsabilità sanzioni |

Approfondimento tematiche specifiche + Casi pratici + Q&A

# T4Data: I webinar di formazione

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

Piattaforma **dedicata** web-based + **Webinar** preregistrati + Materiali di supporto

| Modulo I | Modulo II | Modulo III | Modulo IV |
|---|---|---|---|
| I fondamentali della protezione dati | RPD: Ruoli, responsabilità | Un toolkit per l'RPD (how-to) | Approfondimenti specifici |

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# T4Data: I webinar di formazione

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

Le lezioni sono tenute da dirigenti e funzionari del Garante esperti delle materie trattate.

Sulla piattaforma, oltre ai video-corsi (realizzati dal Garante in house), saranno disponibili le slides presentate dai docenti oltre a eventuali materiali di approfondimento e link utili.

La fruizione dei webinar non prevede procedure di monitoraggio o valutazioni da parte del Garante, anche se saranno messi a disposizione dei test di auto-valutazione per consentire eventualmente ai partecipanti di verificare da sé la comprensione dei contenuti fruiti.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# T4Data: I webinar di formazione

https://www.t4data.dev/login

La partecipazione al corso è riservata agli RPD dei soggetti pubblici i cui nominativi sono stati comunicati attraverso la procedura online attivata sul sito web istituzionale del Garante.

Per accedere ai webinar sarà sufficiente collegarsi all'indirizzo web sopra indicato e digitare le credenziali ricevute all'atto della procedura di comunicazione del nominativo.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

## T4Data

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

GDPR ⟺ G RPD

**Buon lavoro a tutti e grazie**

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# I trattamenti automatizzati e la profilazione: quando i rischi per i diritti e le libertà delle persone sono elevati

Francesco Modafferi

T4DATA


REGIONE
PIEMONTE

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

In collaborazione con REGIONE MARCHE

# Il trattamento dei dati personali per finalità di cura e ricerca

## PROGRAMMA

**9:00 - Registrazione dei partecipanti**

**9:30 - Saluti istituzionali** - Assessore regionale *Fabrizio Cesetti*

**9.45 - Presentazione del progetto T4DATA** - *Antonio Caselli*, Segreteria generale del Garante

**10:00 - Sanità tra tecnologia e gestione del rischio (Valutazione di impatto, DPO e registro delle attività di trattamento)** - *Francesco Modafferi*, Dirigente Dipartimento realtà pubbliche e Dipartimento sanità e ricerca

**10:40 - Presupposti di liceità del trattamento in ambito sanitario: il consenso e l'interesse pubblico** - *Francesca Cecamore*, Dipartimento sanità e ricerca

**11.20 - Pausa**

**11:40 - Regole deontologiche, codici di condotta e misure di garanzia** - *Silvia Melchionna*, Dipartimento sanità e ricerca

**12:20 - La ricerca scientifica, medica biomedica ed epidemiologica** - *Chiara di Somma*, Dipartimento sanità e ricerca

**13:00 – Pausa**

**14:00 - Esame di alcuni casi pratici all'attenzione dell'Autorità relativi alla prima applicazione del RGPD**

**15:00 - Dibattito**

**16:00 - Chiusura dei lavori**

RGPD REGOLAMENTO (UE) 2016/679

**7 giugno 2019**

**Auditorium Tamburi**
**Mole Vanvitelliana**
**Banchina Giovanni da Chio, 28**
**Ancona**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

T4DATA

In collaborazione con
REGIONE CALABRIA

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

# Protezione dei dati personali e trasparenza della PA dopo il Regolamento (UE) 2016/679

## PROGRAMMA

9:00 - Registrazione dei partecipanti

9:30 - Saluti istituzionali - *Gerardo Mario Oliverio*, Presidente della Regione Calabria

9.45 - Presentazione del progetto T4DATA - *Antonio Caselli*, Segreteria generale del Garante

10:00 - Evoluzione del concetto di trasparenza dalla l. 241/1990 al d.lgs. 33/2013 - *Francesco Modafferi*, Dirigente Dip. realtà pubbliche e Dip. sanità e ricerca

10:40 - Obblighi di pubblicazione online da parte delle Pubbliche Amministrazioni e protezione dei dati personali - *Anna Carla Meloni*, Dip. realtà pubbliche

11.20 - Pausa

11:40 - Le indicazioni del Garante su specifici casi di pubblicazione (dichiarazione redditi, curriculum, dati di beneficiari di aiuti economici, albo pretorio online, concorsi e graduatorie) - *Elena Pesaresi*, Dip. realtà pubbliche

12:20 - Accesso civico e protezione dei dati personali - *Miriam Viggiano*, Dip. realtà pubbliche

13:00 - Pausa

14:00 - Pubblicazioni online e accesso civico: esame di casi pratici (scelta dei provvedimenti del Garante più significativi)

15:00 - Risposte ai quesiti

16:00 - Chiusura dei lavori

**Evento riservato ai Responsabili della Protezione dei Dati (RPD) operanti presso i soggetti pubblici**

RGPD

## 26 giugno 2019

Sala Verde della Cittadella regionale
Regione Calabria
Viale Europa
Località Germaneto Catanzaro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

In collaborazione con REGIONE PIEMONTE

# La gestione del rischio e la sicurezza del trattamento

## PROGRAMMA

**9:00 - Registrazione dei partecipanti**

**9:30 - Saluti istituzionali** - *Alberto Cirio*, Presidente della Regione Piemonte

**9.45 - Presentazione del progetto T4DATA** - *Luigi Montuori*, Dirigente Serv. relazioni internazionali e con l'Unione europea

**10:00 - I trattamenti automatizzati e la profilazione: quando i rischi per i diritti e le libertà delle persone sono elevati** - *Francesco Modafferi*, Dirigente Dip. realtà pubbliche e Dip. sanità e ricerca

**10:40 - Privacy by default e by design, la valutazione di impatto, consultazione del Garante e le particolarità della gestione del rischio in ambito pubblico** - *Irene Faganello*, Dip. realtà pubbliche

**11.20 - Pausa**

**11:40 - Accountability e sicurezza dei trattamenti: misure tecnologiche e responsabilità dei titolari** - *Cosimo Comella*, Dirigente Dip. tecnologie digitali e sicurezza informatica

**12:20 - Principio di minimizzazione, anonimizzazione e pseudonimizzazione: tecniche di tutela integrata nel trattamento** - *Giuseppe D'Acquisto*, Dip. tecnologie digitali e sicurezza informatica

**13:00 - Pausa**

**14:00 - Casi pratici di gestione dei data breach: la valutazione del rischio, la notifica al Garante e la comunicazione agli interessati** - *Marco Coppotelli*, Dip. tecnologie digitali e sicurezza informatica

**15:00 - Risposte ai quesiti**

**16:00 - Chiusura dei lavori**


**1° ottobre 2019**

Centro Congressi dell'Unione Industriale di Torino
Via Fanti 17
Torino

# Il nuovo collegio

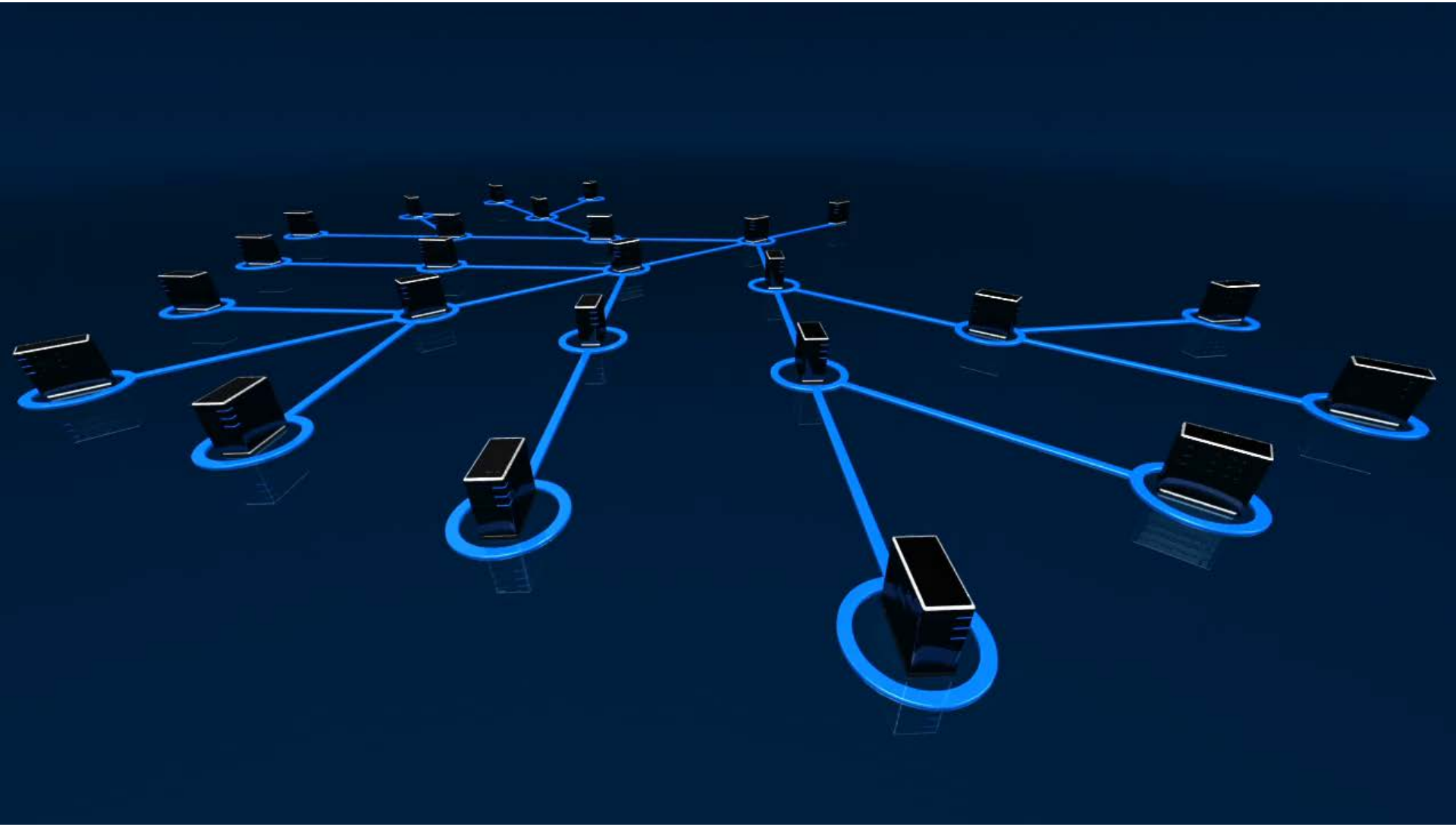
# Di cosa parleremo?

1. I rischi nel trattamento dei dati in ambito pubblico
2. I trattamenti automatizzati e la profilazione
3. Il ruolo (fondamentale) del RPD

# I rischi nel trattamento dei dati in ambito pubblico

Volere fare la frittata, senza rompere le uova

# Un mondo di dati



T4DATA

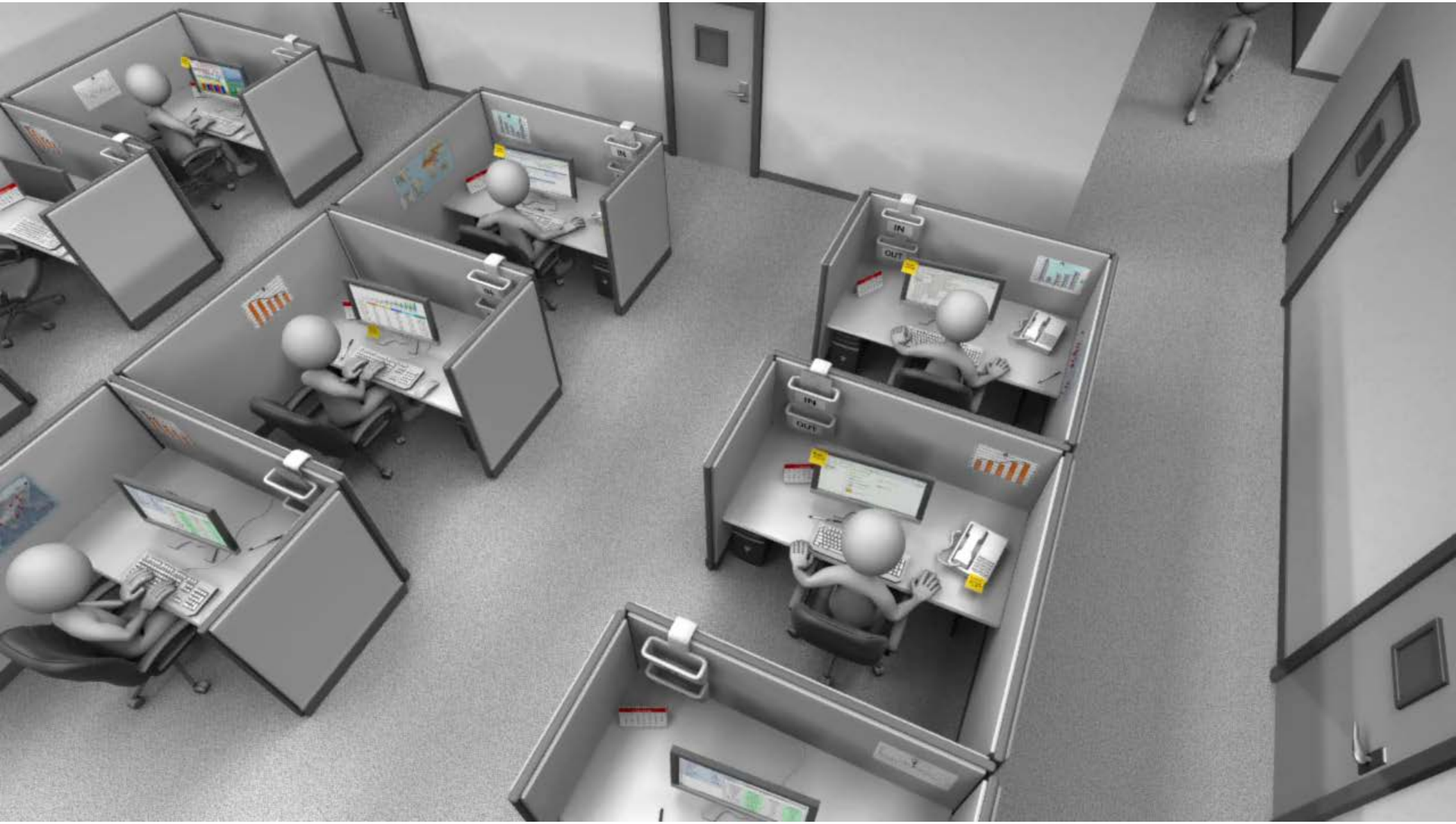
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Big data, ma non per caso


**Le tecnologie  sono configurate per estrarre dati (e quindi valore) dagli utenti più ancora che per soddisfare i loro bisogni.**

**Una volta che tutte le informazioni che ci riguardano sono in mano ad altri la nostra capacità di autodeterminazione viene limitata**

# I trattamenti in «ambito pubblico» non fanno eccezione



# Concetto chiave:

**PROPORZIONALITA'**

Spetta alle norme (diritto dell'Unione o degli Stati membri) il compito di stabilire i casi e i modi in cui un compito svolto nel pubblico interesse o l'esercizio di pubblici poteri possa essere svolto, in qualità di titolare del trattamento, da una autorità pubblica o altra persona giuridica di diritto pubblico o da un soggetto avente natura giuridica privata

Il termine "necessario", comune a molte delle basi giuridiche contenute nell'art. 6 e 9 del Regolamento, deve essere interpretato alla luce del fatto che il concetto di necessità costituisce nel diritto comunitario un elemento consolidato del criterio di proporzionalità

Esso comporta quindi che l'autorità che adotta una misura interferente con un diritto tutelato dall'ordinamento comunitario, per conseguire uno scopo legittimo, deve dimostrare che essa rappresenta la misura meno restrittiva per raggiungere tale scopo

Per la Corte europea dei diritti dell'uomo l'aggettivo "necessario" implica che sussista per lo Stato "*una pressante esigenza sociale*" di agire in un determinato modo e che la misura adottata sia proporzionata al legittimo scopo perseguito

**Trasparenza**

Estensione ai dirigenti degli obblighi di trasparenza previsti per i titolari di incarichi politici

**Statistica**

Censimento permanente e sistema dei registri


**Fisco**

Fatturazione elettronica

**Pubblico impiego**

Rilevazione delle presenze attraverso i dati biometrici

**Previdenza**

Sistema intelligente per la selezione visite fiscali

**Sanità**

Analisi dei dati del servizio sanitario attraverso intelligenza artificiale

# La «dittatura» dell’esponenziale

La velocità esponenziale dell’evoluzione dell’innovazione tecnologica **marginalizza e, alla lunga, annichilisce, il tempo necessario alla comprensione e alla riflessione, privando gli individui e le società del diritto di valutare i fenomeni e di manifestare o meno il loro assenso, in altre parole, li priva del diritto di decidere liberamente delle loro vite.***

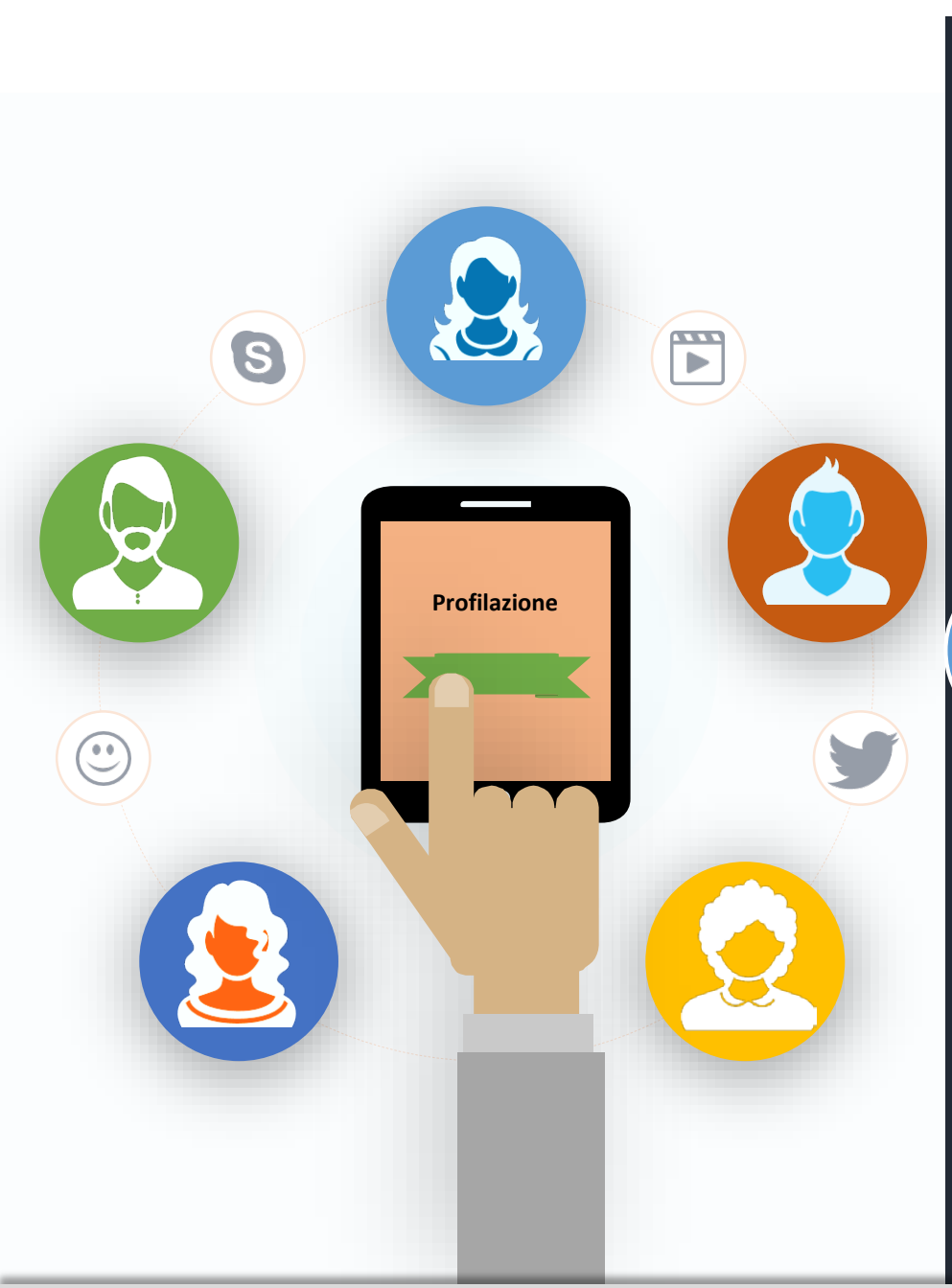
* Eric Sadin Critica della ragione artificiale Luiss

**Il compito della tecnologia non è più soltanto quello di raccogliere dati e organizzarli ma quello di rivelare, in modo automatizzato, la verità dei fenomeni al di là della loro apparenza.**

# Gli effetti collaterali latenti del trattamento


- Come rilevato da Ulrich Beck, l'evoluzione tecnologica va di pari passo con la produzione sociale di rischi; uno degli obiettivi di fondo della regolazione è dunque quello di gestire i cc.dd. "effetti collaterali latenti" di questa evoluzione per "*limitarli e diluirli distribuendoli in modo che non ostacolino il processo di modernizzazione né travalichino i confini di ciò che è considerato* ***'tollerabile'***".
- In questo contesto, poiché sempre più spesso si ricorre, sia in ambito pubblico che privato, ad attività di profilazione e a processi decisionali automatizzati, il Regolamento introduce, al riguardo, nuove **garanzie** per far fronte ai rischi che ne possono derivare.

# I trattamenti automatizzati e la profilazione




Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti

- rendimento professionale
- situazione economica
- salute
- preferenze personali
- interessi
- affidabilità
- comportamento
- ubicazione o spostamenti

La profilazione è una procedura che, impiegata per effettuare previsioni utilizzando dati provenienti da varie fonti, può implicare una serie di deduzioni utili per inferire qualcosa su una persona in base alle qualità di altre persone che sembrano statisticamente simili.

Il Regolamento si è ispirato alla definizione di cui alla raccomandazione CM/Rec (2010)132 del Consiglio d'Europa nella quale si evidenzia che la profilazione normalmente prevede tre fasi distinte:


Come regola generale, se le prime due fasi (*data warehousing e data mining*) possono essere svolte anche mediante l'uso di dati anonimi o pseudonomizzati, la terza fase invece comporta necessariamente dati riferiti a persone identificate o identificabili.

Siamo di fronte a un trattamento di dati complesso dal quale potrebbero derivare **errori di valutazione pregiudizievoli per l'interessato** quali, ad esempio, l'ingiusta privazione di provvidenze o benefici o il mancato accesso a determinati beni o servizi, in violazione del principio di non discriminazione.

Ciò indipendentemente dal fatto che la profilazione possa, in molti casi, produrre effetti utili per le persone e le organizzazioni, offrendo loro vantaggi quali miglioramenti dell'efficienza e risparmi di risorse.

## POSITIVES

- **Vantaggi**
- **Più efficienza**
- **Risparmi**

## NEGATIVES

- **Privazione benefici**
- **Mancato accesso a beni o servizi**

# Diritti rafforzati

- Per questo il Regolamento prevede, innanzi tutto, che gli interessati siano adeguatamente informati (Considerando 60 e 63, nonché artt. 13 e 14).
- Gli art. 13 e 14 prevedono infatti un **obbligo di trasparenza "rafforzato"** che implica, da un lato, che l'interessato sia avvertito circa il fatto che sarà oggetto di un trattamento automatizzato, compresa la sua profilazione, e dall'altro, che sia messo in condizione **di conoscere la logica utilizzata per tale tipo di trattamento e le conseguenze.**
- Ove l'interessato eserciti poi il diritto di accesso previsto dall'art. 15 del Regolamento, **il titolare del trattamento è tenuto a fornire**, oltre alle informazioni generali sul trattamento, anche **indicazioni circa i dati utilizzati per creare il profilo e a consentire l'accesso anche alle informazioni sulla base delle quali l'interessato è stato inserito in un determinato segmento** .

# Limiti del diritto

- Fino a che punto arrivi i diritto dell'interessato a ricevere informazioni significative sulla logica di questa particolare tipologia di trattamenti è questione assai dibattuta in dottrina.
- **Il tema della protezione dei dati si intreccia con quello della tutela del *Know how* e del segreto industriale.**
- Come rilevato infatti dal Considerando n. 63 del Regolamento, l'esercizio del diritto di accesso non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il *software*.
- Tuttavia, il titolare del trattamento non può fare affidamento sulla protezione dei segreti aziendali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato.

## Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione

- L'interessato ha il **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici su di esso o che incida in modo analogo significativamente sulla sua persona** (art. 22, paragrafo 1).
- **Tale previsione configura un vero e proprio divieto generale nei confronti di processi decisionali basati unicamente sul trattamento automatizzato e opera indipendentemente dal fatto che l'interessato intraprenda un'azione in merito.**
- La disposizione, che ricalca sostanzialmente quella riportata all'art. 15 della Direttiva 95/46/CE e all'art. 14 del Codice in materia di protezione dei dati personali (prima della revisione apportata dal d.lgs. n. 101/2018), nasce dalla "*necessità di sottrarre la persona dalla 'dittatura dell'algoritmo' emblema di una società della spersonalizzazione, nella quale scompare la persona del decisore, sostituito appunto da procedure automatizzate*" (Stefano RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli)*.

- L’art. 22, paragrafo 1, si riferisce a decisioni “basate unicamente” sul trattamento automatizzato, quindi senza alcun coinvolgimento umano nel processo decisionale. **Come sottolineato dal Gruppo art. 29, per aversi un coinvolgimento umano è necessario che il controllo sulla decisione sia significativo e non costituisca un semplice gesto simbolico.**
- Quando il trattamento automatizzato non è necessario per la conclusione o l’esecuzione di un contratto tra l’interessato e un titolare del trattamento, ovvero non si basa sul consenso esplicito dell’interessato, il processo decisionale automatizzato e la profilazione, sono ammessi nei casi in cui il diritto dell’Unione o dello Stato membro ne autorizzi l’uso.
- **Quando la profilazione è necessaria per l’esecuzione di un compito di interesse pubblico (art. 6, paragrafo 1, lettera e), è necessario quindi che la base giuridica (norma di legge o di regolamento) indichi esplicitamente la possibilità di utilizzare tecniche di profilazione e preveda anche misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato**

# L'accesso all'algoritmo secondo il Giudice amministrativo

- In un contesto diverso dalla protezione dei dati personali, è interessante rilevare come l'uso di algoritmi, da parte dell'amministrazione pubblica, abbia recentemente impegnato anche il giudice amministrativo chiamato a valutare l'ammissibilità del diritto di accesso *ex* art. 22 della legge n. 241/1990 al Codice sorgente di un algoritmo.
- **Nel caso di specie, il diritto all'accesso è stato riconosciuto dal giudice adito in quanto il procedimento amministrativo era stato gestito in modo automatico e per mezzo di un complesso sistema informatico e tutte le decisioni rilevanti erano state assunte esclusivamente attraverso l'algoritmo**.
- Secondo il giudice, consegnare ai richiedenti la mera descrizione del funzionamento dell'algoritmo non assolveva alla medesima funzione conoscitiva data dall'acquisizione diretta del linguaggio informatico sorgente (Tar del Lazio, sezione III *bis*, n. 03742/2017 del 14 febbraio 2017 ).

**Ragioni di trasparenza, tanto del procedimento amministrativo che del trattamento dei dati personali, inducono, in linea di principio, a garantire agli interessati, nell'ambito pubblico, l'accesso alle informazioni rilevanti sul funzionamento dei sistemi automatizzati di decisione e dei sistemi di profilazione .**

# Diritto d'autore

- Nella sentenza si affronta anche il tema del rapporto con la tutela del diritto di autore e di proprietà intellettuale rilevando che "*né il diritto di autore né la proprietà intellettuale precludono la semplice riproduzione, ma precludono, invece, al massimo, soltanto la riproduzione che consenta uno sfruttamento economico e, non essendo l'accesso lesivo di tale diritto all'uso economico esclusivo dell'opera, l'ostensione deve essere consentita nelle forme richieste da parte dell'interessato, ossia della visione e dell'estrazione di copia,* ***fermo restando che delle informazioni ottenute dovrà essere fatto un uso appropriato, ossia esclusivamente un uso funzionale all'interesse fatto valere con l'istanza di accesso che, per espressa allegazione della parte ricorrente, è rappresentato dalla tutela dei diritti dei propri affiliati****, in quanto ciò costituisce non solo la funzione per cui è consentito l'accesso stesso, ma nello stesso tempo anche il limite di utilizzo dei dati appresi, con conseguente responsabilità diretta dell'avente diritto all'accesso nei confronti del titolare del software*".

# Tar Lazio

- *Le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione,* ***non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere e che pertanto, al fine di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il dominus del procedimento stesso, all'uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt'oggi un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo;***
- *ostando alla deleteria prospettiva orwelliana di dismissione delle redini della funzione istruttoria e di abdicazione a quella provvedimentale, il presidio costituito dal baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo*"

- Sentenze del 10 settembre 2018 (n. 09224, n. 09225, n. 09226, n. 09227, n. 09228, n. 09229

# Consiglio di Stato

- In generale, **non può essere messo in discussione che un più elevato livello di digitalizzazione dell'amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti**. L'utilità di tale modalità operativa di gestione dell'interesse pubblico è particolarmente evidente con riferimento a procedure seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale.
- Ciò è, invero, conforme ai canoni di efficienza ed economicità dell'azione amministrativa (art. 1 l. 241/90), i quali, secondo il principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.), impongono all'amministrazione il conseguimento dei propri fini con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale.
- **In altre parole, l'assenza di intervento umano in un'attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica.**

# Consiglio di Stato

**L'utilizzo di procedure "robotizzate" non può, tuttavia, essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa.**

Difatti, la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima, anche se ciò avviene in via esclusiva. Questa regola algoritmica, quindi:

- **possiede una piena valenza giuridica e amministrativa**, anche se viene declinata in forma matematica, e come tale, deve soggiacere ai principi generali dell'attività amministrativa, quali quelli di pubblicità e trasparenza (art. 1 l. 241/90), di ragionevolezza, di proporzionalità, etc.;
- **non può lasciare spazi applicativi discrezionali** (di cui l'elaboratore elettronico è privo), ma deve prevedere con ragionevolezza una soluzione definita per tutti i casi possibili, anche i più improbabili;
- **vede sempre la necessità che sia l'amministrazione a compiere un ruolo ex ante di mediazione e composizione di interessi,** anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo (soprattutto nel caso di apprendimento progressivo e di deep learning);
- **deve contemplare la possibilità che sia il giudice a "dover svolgere, per la prima volta sul piano umano, valutazioni e accertamenti fatti direttamente in via automatica",** con la conseguenza che la decisione robotizzata "impone al giudice di valutare la correttezza del processo automatizzato in tutte le sue componenti".

# Consiglio di Stato

Ciò comporta un duplice ordine di conseguenze.

- In primo **luogo il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico.**
- In secondo luogo**, la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo.**

In questo senso, la decisione amministrativa automatizzata impone al giudice di valutare in primo luogo la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione. Da qui, come si è detto, si conferma la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo.

In secondo luogo, conseguente al primo, il giudice deve poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo, di cui si è ampiamente detto.

# La regolazione dell'algoritmo

- La delicatezza del tema e delle conseguenze non può essere sottovalutata se solo si pensa che, come è stato giustamente osservato, "*la società ha accumulato millenni di esperienza nella comprensione e nello studio del comportamento umano. Ma come si fa a regolamentare un algoritmo?*" (V. MAYER SHÖNBERGERER, K. CUKIER in *Big data – una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*).
- Se da un lato è inevitabile che, in una società complessa caratterizzata da un'estrema velocità dei cambiamenti culturali e sociali, anche il soggetto pubblico utilizzi strumenti tecnologicamente avanzati nell'elaborazione di enormi quantità di dati, dall'altro diventa di fondamentale importanza "la verificabilità del processo di analisi" a tutela del cittadino il quale può subire gravissimi danni per effetto dell'esercizio, sempre più automatizzato, del potere pubblico.

# Il ruolo (fondamentale) del RPD

## L’art. 38 del Regolamento

Il Regolamento dedica alcune specifiche disposizioni per definire la posizione del RPD e prevede che:

- **riferisce direttamente al vertice gerarchico** del titolare o del responsabile del trattamento;
- il titolare e il responsabile del trattamento si assicurano che **il RPD non riceva alcuna istruzione** per quanto riguarda l’esecuzione di tali compiti;
- **non è rimosso o penalizzato** per l’adempimento dei propri compiti.

## Il coinvolgimento

Il titolare e il responsabile del trattamento si assicurano che il RPD sia **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.

**Potrebbe essere opportuno definire delle linee guida interne per stabilire i casi nei quali il RPD debba essere consultato**

# Indipendenza (Cons. 97)

I RPD, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in **maniera indipendente**.

**Il parere del RPD – e ogni azione intrapresa contro questo parere – devono essere registrati e possono essere utilizzati contro il titolare o il responsabile in caso di indagine da parte delle relative autorità di protezione dei dati** (come già visto, al contrario, il fatto che un titolare o un responsabile agiscano in accordo con il parere o gli orientamenti del RPD può essere considerato un "elemento" per la dimostrazione della conformità al RGPD - Considerando 77)

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

## Gli elementi che possono indebolire la posizione del RPD

- **un RPD part-time** vive un conflitto permanente le sue funzioni di RPD e le funzioni in un altro ambito. Per quanto riguarda gli sviluppi di carriera e gli obiettivi raggiunti, l'organizzazione potrebbe **attribuire un gran peso alle attività non legate ai compiti di RPD**; le altre attività potrebbero comportare responsabilità dirette in caso di omissioni o ritardi che potrebbero relegare i compiti da RPD in secondo piano. Un RPD a tempo parziale corre anche il rischio di ritrovarsi in una situazione di conflitto di interessi;
- un **RPD con un contratto a termine** è in una posizione più debole nell'espletamento delle sue funzioni rispetto a un RPD con un contratto a tempo indeterminato. Il timore potrebbe essere quello che l'espletamento delle proprie funzioni possa avere un impatto negativo sul rinnovo contrattuale;
- un **RPD che riporta a, ed è valutato da, un diretto superiore gerarchico**, può sentirsi spinto a fare gioco di squadra e per questo a non contrastare colleghi e superiori, magari pensando che un'attitudine più intransigente per quanto riguarda i compiti legati alle funzioni di RPD possano avere un impatto negativo sulla sua carriera;
- un RPD che ha la **necessità di richiedere personale e risorse (risorse IT, un bilancio per viaggi e formazioni) al suo diretto superiore** gerarchico può essere in difficoltà se costui non è pienamente coinvolto nel raggiungimento della conformità della protezione dei dati

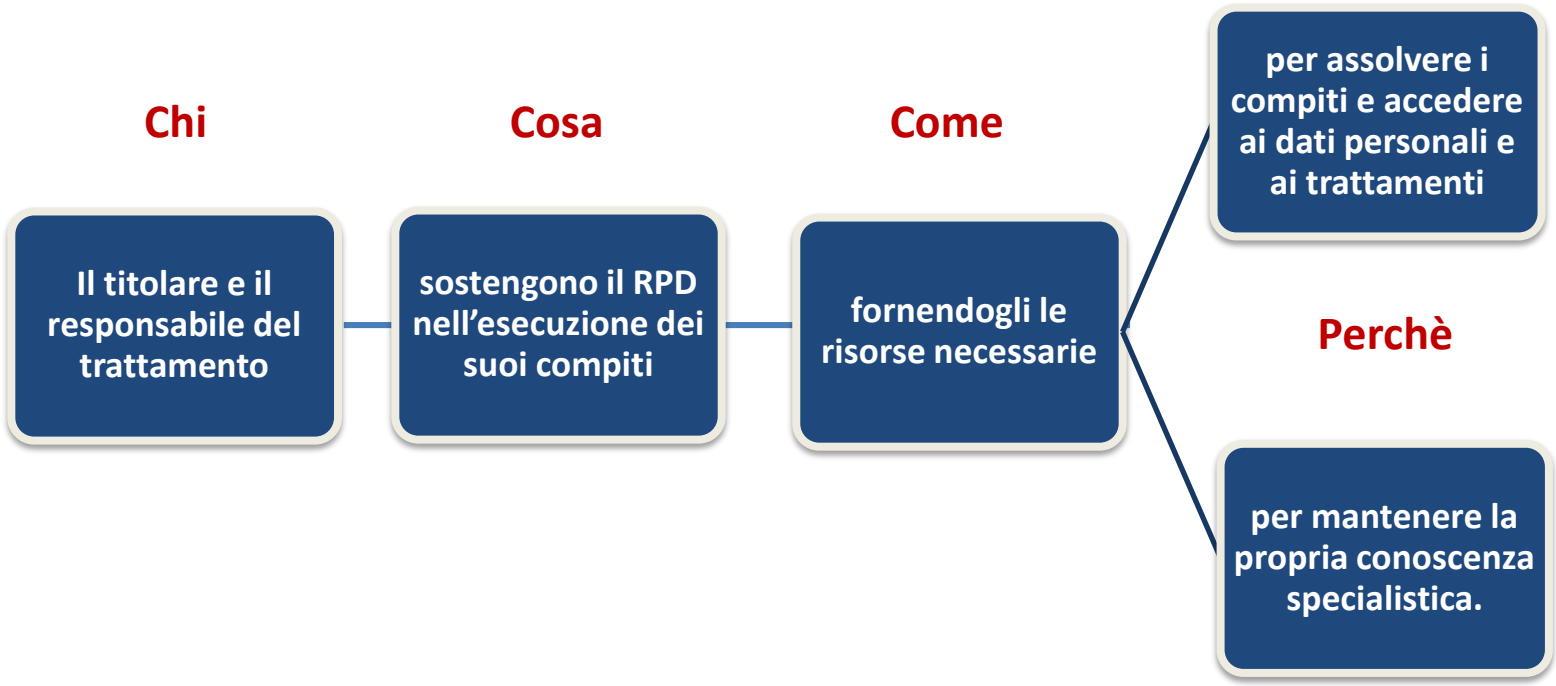
## Troppi compiti designazione non idonea

Posizione

L'insieme degli argomenti sopra riportati, considerati anche alla luce della complessità della struttura organizzativa, l'elevato numero di cittadini/interessati che possono rivolgersi al RPD "*per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti*" (art. 38, par. 4 del Regolamento), la numerosità dei trattamenti posti in essere, nonché la rete di responsabili del trattamento/società cui codesto ente ricorre per lo svolgimento dei trattamenti di dati personali nell'ambito dei propri compiti istituzionali, dovrebbe suggerire a codesta Amministrazione di affidare l'incarico di RPD a una persona che possa dedicarsi a tempo pieno a tale incarico e al quale siano assegnate risorse adeguate. Ciò, in particolare, alla luce delle notevoli criticità già rilevate dall'Autorità nell'ambito di diversi procedimenti ancora in corso.

Si rammenta, in ogni caso, che l'inosservanza delle disposizioni di cui agli artt. 37-39 del Regolamento comporta l'applicazione della sanzione amministrativa pecuniaria di cui all'art. 83, par. 4, lett. *a*) del Regolamento e che "*il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento.*

# Risorse


Chi
Cosa
Come
Il titolare e il responsabile del trattamento
sostengono il RPD nell'esecuzione dei suoi compiti
fornendogli le risorse necessarie
Perchè
per assolvere i compiti e accedere ai dati personali e ai trattamenti
per mantenere la propria conoscenza specialistica.

# Risorse

tempo sufficiente per l'espletamento dei compiti affidati

supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale

comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note

accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali

formazione permanente

alla luce delle dimensioni e della struttura dell'ente può risultare necessario costituire un ufficio o un gruppo di lavoro RPD

**Quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD.**

**La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.**

# Mai dimenticarsi di avere un ruolo di garanzia

L'autorità di controllo e i RPD danno vita ad un "partenariato strategico":

→ le DPA incoraggiano gli interessati (in primo luogo e soprattutto) a risolvere eventuali problemi direttamente con i RPD;

↓

i RPD devono essere in grado – ed hanno il compito – di collaborare con l'Autorità per garantire che le risposte alle domande e ai reclami siano gestite in modo corretto e producano, se del caso, i cambiamenti necessari nelle prassi del titolare.

→ Le DPA devono poter fare affidamento sui RPD e sulla loro capacità di essere al fianco degli interessati per qualsiasi reclamo.

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# *Privacy by default* e *by design*, la valutazione di impatto, consultazione del Garante e le particolarità della gestione del rischio in ambito pubblico

**Dott.ssa Irene Faganello**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# ARGOMENTI TRATTATI

1. **Alcuni concetti fondamentali per la gestione del rischio in ambito pubblico: rischio, *privacy by design* e *by default***

2. **La valutazione di impatto: cos'è e quando è obbligatoria**

3. **Il contenuto della valutazione di impatto**

4. **I casi di consultazione del Garante**

5. **Il rischio elevato in ambito pubblico (art. *2-quinquiesdecies del Codice)*.**

GDPR
GENERAL
DATA PROTECTION
REGULATION

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Il concetto di rischio

## *RISCHIO*


L.G. Gruppo Art. 29
«Per "**rischio**" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini
di gravità e probabilità» per i diritti e le libertà

**fonti** di rischio

**impatti potenziali** sui diritti e le libertà degli interessati

**minacce**

**probabilità** e **gravità**

*Linee-guida del 4/10/2017 (WP 248)*

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Valutazione del rischio

***RISCHIO***

rischi prodotti dal trattamento con probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

art. 24


Non solo rischi derivanti da una possibile violazione di dati personali

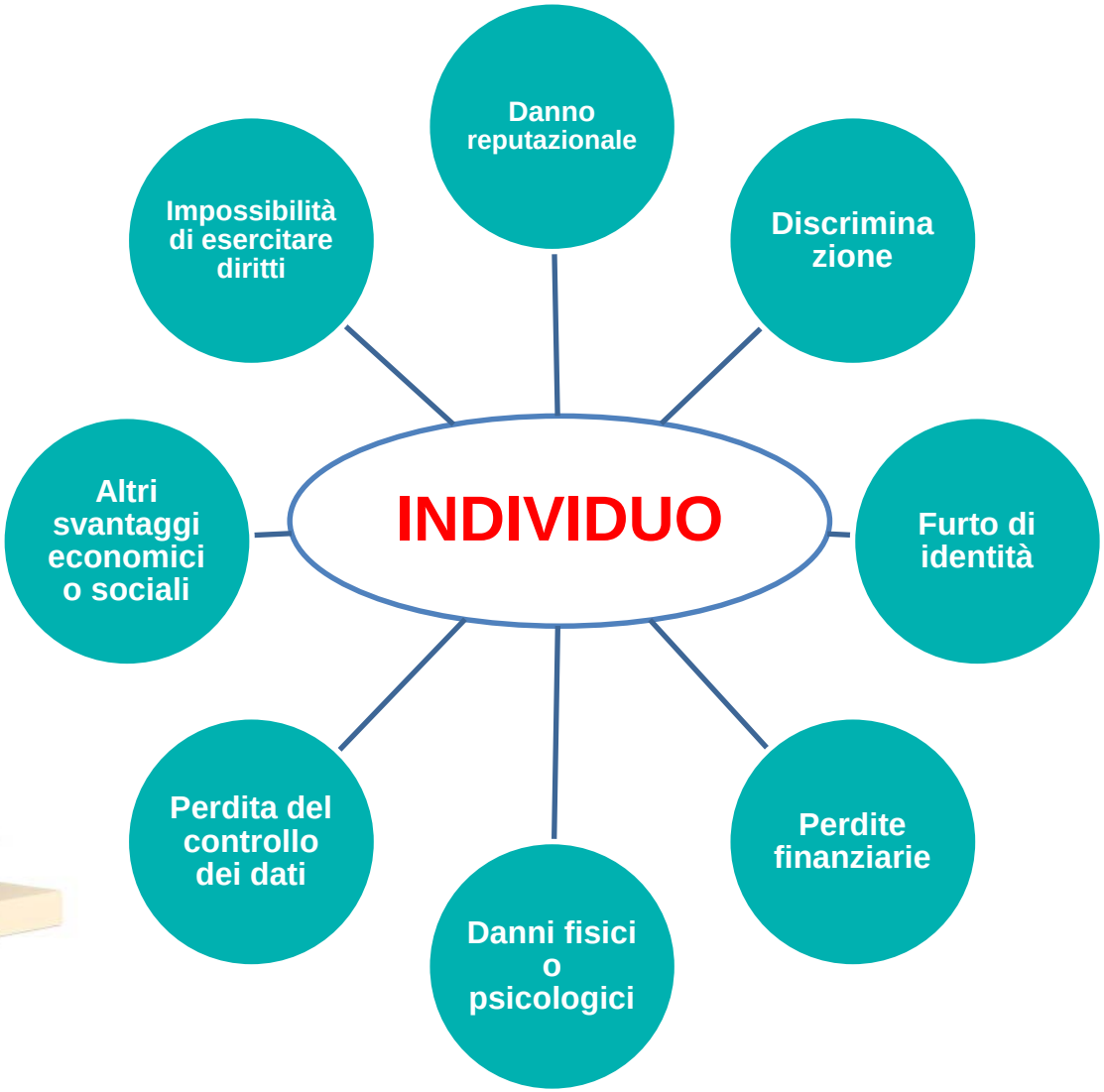
**Trattamento nel suo complesso**

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Valutazione del rischio

## *RISCHIO*

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# «*Privacy by design* e *by default*»
# Protezione dei dati fin dalla progettazione e per impostazione predefinita
# art. 25

## Il Titolare del trattamento

misure
**TECNICHE E**
**ORGANIZZATIVE**

*by design*

*by default*

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Protezione dei dati fin dalla progettazione
# *privacy by design*
# art. 25, par. 1

## Il Titolare del trattamento

mette in atto misure **TECNICHE** E **ORGANIZZATIVE** adeguate (pseudonimizzazione) volte a

**ATTUARE** in modo efficace **i principi** di protezione dei dati (minimizzazione)

**INTEGRARE** nel trattamento le **necessarie garanzie** per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Protezione dei dati fin dalla progettazione
# *privacy by design*
# art. 25, par. 1

## Il Titolare del trattamento

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Protezione dei dati fin dalla progettazione
# *privacy by design*
# art. 25, par. 1

**Quando**

al momento di determinare i mezzi del trattamento

e all'atto del trattamento

misure tecniche e organizzative adeguate e garanzie

# Protezione per impostazione predefinita
# *privacy by default*
# art. 25, par. 2

## Il Titolare del trattamento

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Protezione per impostazione predefinita *privacy by default* art. 25, par. 2

## Il Titolare del trattamento

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# protezione per impostazione predefinita
# *privacy by default*
# art. 25, 2

## Il Titolare del trattamento


**Impostazione obbligatoria per**

- **la quantità dei dati personali 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 fisiche senza l'intervento della persona fisica

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Valutazione d'impatto sulla protezione dei dati (DPIA) art. 35


## Rischio elevato

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Valutazione d'impatto sulla protezione dei dati (DPIA) art. 35


Quando il trattamento presenta un **rischio elevato** per i diritti e le libertà delle persone fisiche è necessario effettuare una **valutazione dell'impatto** sulla protezione dei dati personali

ed eventuale **consultazione preventiva** del Garante

in particolare, uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Valutazione d'impatto sulla protezione dei dati (DPIA) art. 35

**Strumento di gestione del rischio elevato**


Misure

↓

Meccanismi

↓

Garanzie

↓

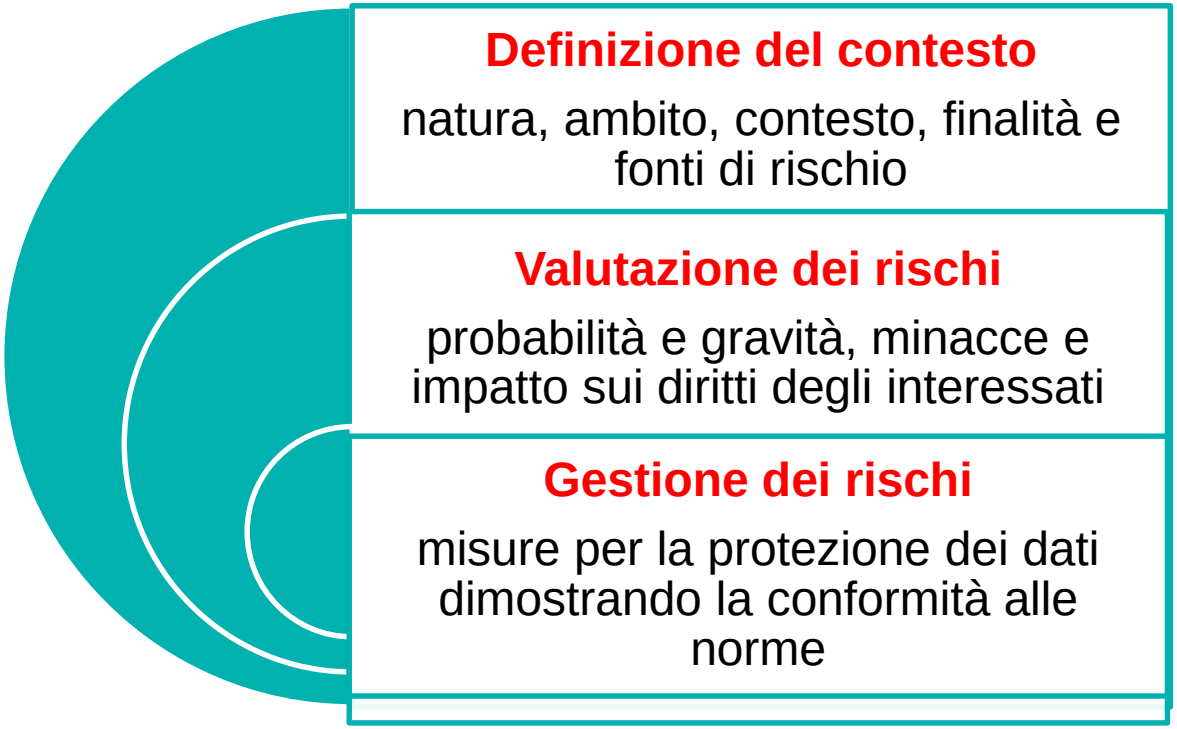
Attenuazione del rischio

Assicurando la protezione dei dati

Dimostrando la conformità al Regolamento

# Valutazione d'impatto sulla protezione dei dati (DPIA) art. 35

***RISCHIO ELEVATO***



# Valutazione d'impatto sulla protezione dei dati (DPIA)
# art. 35

**Per il trattamento che presenta un rischio elevato per i diritti e le libertà delle persone fisiche è necessario effettuare una valutazione d'impatto/DPIA**

## QUANDO?


**elenco non tassativo**
**casi obbligatori espressi**
**DPIA**
(art. 35, comma 3)

# Casi di valutazione d'impatto obbligatoria art. 35, 3

valutazione sistematica e globale di aspetti personali …

… basata su trattamento automatizzato

sulla quale si fondano decisioni che …

… hanno effetti giuridici o incidono significativa-mente sulle persone fisiche

es: profilazione

# Casi di valutazione d'impatto obbligatoria
## trattamenti su larga scala di particolari categorie di dati
## art. 35, 3

DATI GENETICI

CONVINZIONI RELIGIOSE(o filosofiche)


OPINIONI POLITICHE


DATI SULLA SALUTE

ORIGINE RAZZIALE O ETNICA

APPARTENENZA SINDACALE


DATI BIOMETRICI

VITA O ORIENTAMENTO SESSUALE

CONDANNE PENALI E REATI

# Casi di valutazione d'impatto obbligatoria art. 35,3

Sorveglianza sistematica su larga scala di una zona accessibile al pubblico





# Altri casi di valutazione d'impatto obbligatoria art. 35, 3

Principio di carattere generale
**RISCHIO ELEVATO**

**NOVE CRITERI**

Linee-guida del 4/10/2017 (WP 248) concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, fatte proprie dal Comitato

# Criteri per l'individuazione del rischio elevato

Principio di carattere generale
**RISCHIO ELEVATO**
*(9 criteri individuati dalle Linee guida)*

- **Trattamenti valutativi o di *scoring*** (affidabilità, rendimento, situazione economica)
- **Decisioni automatizzate che producono significativi effetti giuridici o analoghi** (benefici, discriminazione)
- **Monitoraggio sistematico**
- **Dati sensibili o dati di natura estremamente personale** (vita familiare, dati finanziari, ubicazione)
- **Trattamenti di dati su larga scala** (numero di interessati, volume, durata e ambito geografico)
- **Combinazione o raffronto di insiemi di dati** (diverse finalità, titolari distinti)
- **Dati relativi a interessati vulnerabili** (squilibrio i poteri tra interessato e titolare, ad es. minori o disabili)
- **Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative**
- **Trattamenti che, di per sé, impediscono di esercitare un diritto o di avvalersi di un servizio o di un contratto**

## art. 35, 4-6
## Casi di valutazione d'impatto privacy obbligatoria

ELENCHI REDATTI DAL GARANTE

- l'Autorità di controllo redige e rende pubblico un **elenco delle tipologie di trattamenti per cui la DPIA è obbligatoria**
- l'Autorità di controllo può redigere e rendere pubblico **un elenco delle tipologie di trattamenti per le quali non è richiesta una DPIA** (facoltativo)


entrambi comunicati al
**Comitato europeo per la protezione dei dati**
adozione del **meccanismo di coerenza** per attività con effetti sulla libera circolazione dei dati personali all'interno dell'Unione

## Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

*Provvedimento del Garante n. 467 dell'11 ottobre 2018 (art. 35, comma 4)*

1. **Trattamenti valutativi o di *scoring* su larga scala**, nonché trattamenti che comportano la **profilazione** degli interessati nonché lo svolgimento di **attività predittive** effettuate anche on-line o attraverso app, relativi ad *"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 dell'interessato*".

2. Trattamenti **automatizzati** finalizzati ad assumere decisioni che producono "***effetti giuridici***" oppure che incidono "***in modo analogo significativamente***" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

3. Trattamenti che prevedono un **utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati**, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

## Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto – Provvedimento del Garante n. 467 dell'11 ottobre 2018 (art. 35, comma 4)

4. Trattamenti su **larga scala** di dati aventi **carattere estremamente personale** (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del **rapporto di lavoro mediante sistemi tecnologici** (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un **controllo a distanza** dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti **non occasionali** di dati relativi a **soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

## Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto – Provvedimento del Garante n. 467 dell'11 ottobre 2018 (art. 35, comma 4)

7. Trattamenti effettuati attraverso l'uso di **tecnologie innovative**, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .

8. Trattamenti che comportano lo **scambio tra diversi titolari di dati su larga scala con modalità telematiche**.

9. Trattamenti di dati personali effettuati mediante **interconnessione, combinazione o raffronto di informazioni**, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

## Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto – Provvedimento del Garante n. 467 dell'11 ottobre 2018 (art. 35, comma 4)

9. Trattamenti di **categorie particolari** di dati ai sensi dell'art. 9 oppure di dati relativi a **condanne penali e a reati** di cui all'art. 10 **interconnessi** con altri dati personali raccolti per **finalità diverse**.

10. Trattamenti **sistematici di dati biometrici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

11. Trattamenti **sistematici di dati genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

Principio di carattere generale
**RISCHIO ELEVATO**

**In caso di dubbio**

Se la necessità non emerge con chiarezza, il Gruppo art. 29 raccomanda di farvi comunque ricorso

**Mancata conduzione**

In caso di mancata conduzione della DPIA, motivare e documentare la scelta, allegando o annotando il parere del RPD

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

## Non è necessaria se:

*L.G. Gruppo Art. 29*

- la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è **già** stata **condotta** una **DPIA**
- il trattamento è stato **sottoposto a verifica** da parte di un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche
- un trattamento trova la propria base legale nel diritto dell'Ue o di uno Stato membro, che disciplina lo specifico trattamento, ed è **già stata condotta una DPIA all'atto della sua definizione,** tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi
- il trattamento **è compreso nell'elenco** dei trattamenti per i quali non è necessario procedere alla DPIA (art. 35, par. 5)

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

## CHI

Il **titolare del trattamento**
che si consulta con
il responsabile della protezione dei dati
(qualora ne sia designato uno)

Il RPD ne sorveglia lo svolgimento

Il responsabile del trattamento deve assistere il titolare nella conduzione della DPIA, fornendo ogni informazione necessaria

La conduzione materiale della DPIA può essere affidata anche a un altro soggetto (interno o esterno), ma la responsabilità ricade sul titolare

## Valutazione d'impatto sulla protezione dei dati (DPIA)
## Art. 35

# QUANDO

**Prima** di procedere al trattamento

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi

Anche per trattamenti in corso per i quali siano intervenuti variazioni di rischio (L.G. Gruppo Art. 29)

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

## COME

***Processo iterativo generale*** *per la conduzione di una DPIA*
*L.G. Gruppo Art. 29*


# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

## *Processo dinamico*

**Se necessario**, il titolare del trattamento procede a un **riesame** per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento (afrt. 35, par. 11)

In termini di buone prassi, per i trattamenti in corso dovrebbe essere previsto un riesame continuo della DPIA, **ripetendo la valutazione a intervalli regolari**

# PUBBLICAZIONE DPIA

Non c'è un obbligo di pubblicare, sarebbe opportuno pubblicarne una sintesi per favorire un rapporto fiduciario

La DPIA va comunque inviata al Garante in caso di consultazione preventiva e a richiesta per consentire gli obblighi di vigilanza

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

*Elementi*


## 1) Descrizione sistematica del trattamento

(art. 35, paragrafo 7, lettera a) )

- si tiene conto della **natura**, dell'**ambito**, del **contesto** e delle **finalità** del trattamento;
- **tipologie di dati** personali oggetto del trattamento, modalità di raccolta, destinatari e periodo previsto di conservazione dei dati stessi;
- la **base giuridica** del trattamento
- **descrizione** funzionale del trattamento;
- **strumenti** coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
- **codici di condotta** approvati (art. 35, paragrafo 8).

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

*Elementi*

## 2) Valutazione di necessità e proporzionalità del trattamento

(art. 35, paragrafo 7, lettera b) )

- **finalità** specifiche, esplicite e legittime (art. 5, par. 1, lett. *b)*);
- **liceità** del trattamento (art. 6);
- dati **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alla finalità del trattamento (art. 5, par. 1, lett. *c)*);
- periodo limitato di **conservazione** (art. 5, par. 1, lett. *e)* ).

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

*Elementi*

## 3) Valutazione dei rischi per i diritti e le libertà degli interessati

(art. 35, paragrafo 7, lettera c))


Origine, natura, particolarità e gravità dei **rischi** o, in modo più specifico, di **ogni singolo rischio** (es. accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:

- si tiene conto delle **fonti di rischio**;
- si identificano gli **impatti potenziali** sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;
- si identificano le **minacce** che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
- si stimano **probabilità** e **gravità**.

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

*Elementi*

## 4) Misure previste per affrontare i rischi
(art. 35, paragrafo 7, lettera d))


- misure previste per gestire i rischi:
  - garanzie, **misure di sicurezza** e **meccanismi** per garantire la protezione dei dati personali e **dimostrare** la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
- misure che contribuiscono ai diritti degli interessati:
  - **informazioni** fornite agli interessati, garanzie per il diritto di **accesso** e **portabilità** dei dati, diritto di **rettifica** e **cancellazione,** diritto di opposizione e limitazione del trattamento;
  - rapporti i **responsabili** del trattamento (art. 28);
  - garanzie per i **trasferimenti** internazionali di dati (Capo V);
  - **consultazione preventiva** (art. 36).

# Valutazione d'impatto sulla protezione dei dati (DPIA)
# Art. 35

*Elementi*

## 5) Coinvolgimento figure rilevanti

- Consulenza **RPD** (art. 35, par. 2), e di altre figure necessarie per lo svolgimento di una DPIA adeguata (responsabili del trattamento, responsabile della sicurezza informatica ecc.)
- Opinioni degli **interessati**, o dei loro rappresentanti (art. 35, par. 9)


## 6) Documentazione delle decisioni assunte

## Prime indicazioni del Garante sulla valutazione di impatto (provv. n. 511 del 20 dicembre 2018)

- La valutazione d'impatto sulla protezione dei dati deve tenere conto dei rischi incombenti sui diritti e sulle libertà degli interessati, anche non riferibili alla fattispecie degli incidenti informatici, esaminando, in modo esaustivo, i diversi scenari di rischio e i possibili impatti al fine di individuare misure adeguate ad affrontarli, annullandoli o, quantomeno, riducendoli a un livello accettabile.

- Non deve risultare focalizzata su aspetti meramente tecnici del trattamento, risultando un documento di valutazione del rischio informatico incombente sui dati.

- Occorre evitare di sfruttare schemi standard e semplificazioni che rischiano di comprometterne l'efficacia, fornendo alla stessa un connotato di eccessiva genericità e, quindi, di inadeguatezza, in relazione all'analisi dei rischi che ne costituisce il presupposto essenziale.

# Consultazione preventiva del Garante
## art. 36, 1

## *RISCHI RESIDUALI ELEVATI*


Qualora la valutazione d'impatto sulla protezione dei dati
indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio

# Consultazione preventiva del Garante
## art. 36, 1

Il Garante, in caso di violazioni del regolamento
e, in particolare,
qualora il titolare non abbia identificato o attenuato sufficientemente il rischio


PARERE SCRITTO

può avvalersi in ogni caso dei poteri di cui all'articolo 58 (es.: rich. info, ispezioni, ingiunzioni, divieti, limitazioni del trattamento, ecc.)

# Consultazione preventiva del Garante sugli atti legislativi e regolamentari

## art. 36, 4

Obbligo di consultazione preventiva del Garante sugli atti legislativi e misure regolamentari che incidono sul trattamento dei dati personali (art. 36, par. 4)

DPIA

**PARERE**

Art 154, comma 5, del Codice

# Autorizzazione del Garante per trattamenti a rischio elevato per l'esecuzione di un compito di interesse pubblico art. 36, 5

**art. 36, 5 del Regolamento**
Il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione di un compito di interesse pubblico.

**AUTORIZZAZIONE ex**
**art. 2-quinquesdecies del Codice**
(art. 36, par. 5 del Regolamento)

DPIA

**Prescrivere misure e accorgimenti anche**
**provvedimenti di carattere generale**
(es. provvedimenti adottati in materia fiscale, reddito di cittadinanza, censimento)

# SANZIONI

(art. 83, 4)


1. mancato rispetto art. 25
2. svolgimento della DPIA quando il trattamento è soggetto a tale valutazione
3. svolgimento non corretto di una DPIA
4. mancata consultazione dell'autorità di controllo competente ove ciò sia necessario
5. violazione art. 2-quinquiesdecies del Codice

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Grazie

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# Pseudonimizzazione, minimizzazione, anonimizzazione. Tutele integrate nel trattamento

**Giuseppe D'Acquisto**

# Pseudonimizzazione (art. 4.5)

**trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Pseudonimizzazione (art. 4.5)

**trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**

Mario

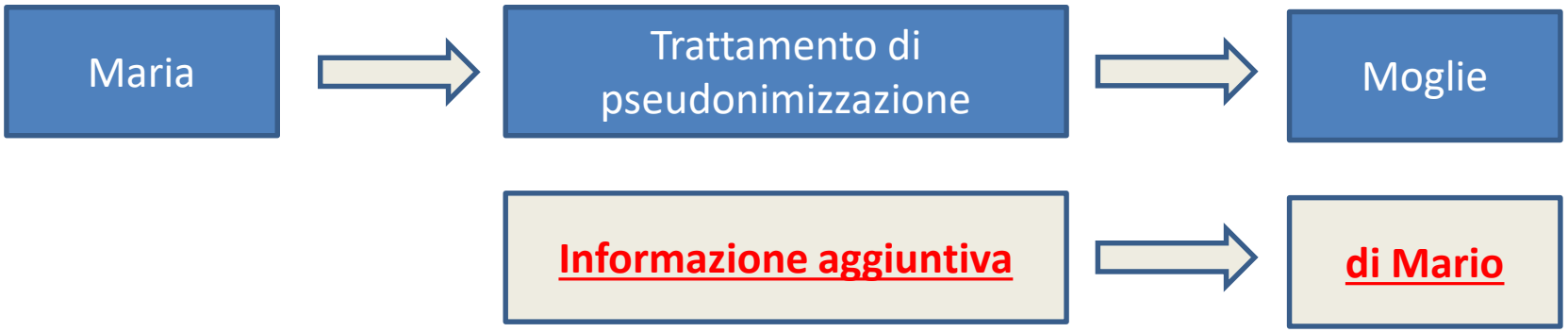
Maria

# Pseudonimizzazione (art. 4.5)

**trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**

# Pseudonimizzazione (art. 4.5)

**trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**



# Pseudonimizzazione (art. 4.5)

**trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**

Mario

Maria

Moglie di Mario

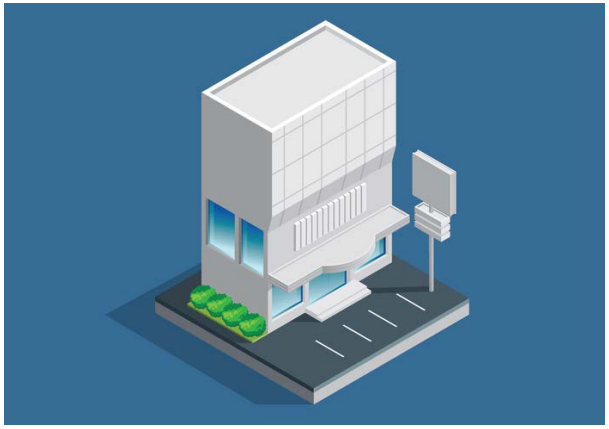
# L’importanza del contesto

Ufficio di Maria

Chi ha scritto questo documento?

- **Maria**
- Moglie di Mario

Ufficio di Mario



Chi è la signora in questa foto?

- Maria
- **Moglie di Mario**

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Pseudonimizzazione: prime considerazioni

Ognuno di noi ha molteplici identità, in ragione del contesto in cui opera

La pseudonimizzazione serve per costruire queste identità. Introduce un principio di relatività delle identità

La pseudonimizzazione non è una forma di anonimizzazione

La pseudonimizzazione non serve (soltanto) a ridurre il potere identificativo del dato

L'informazione aggiuntiva può essere nelle mani del titolare o dell'interessato

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Scopo della pseudonimizzazione (art. 25)

**Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.**

***…pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing…***

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

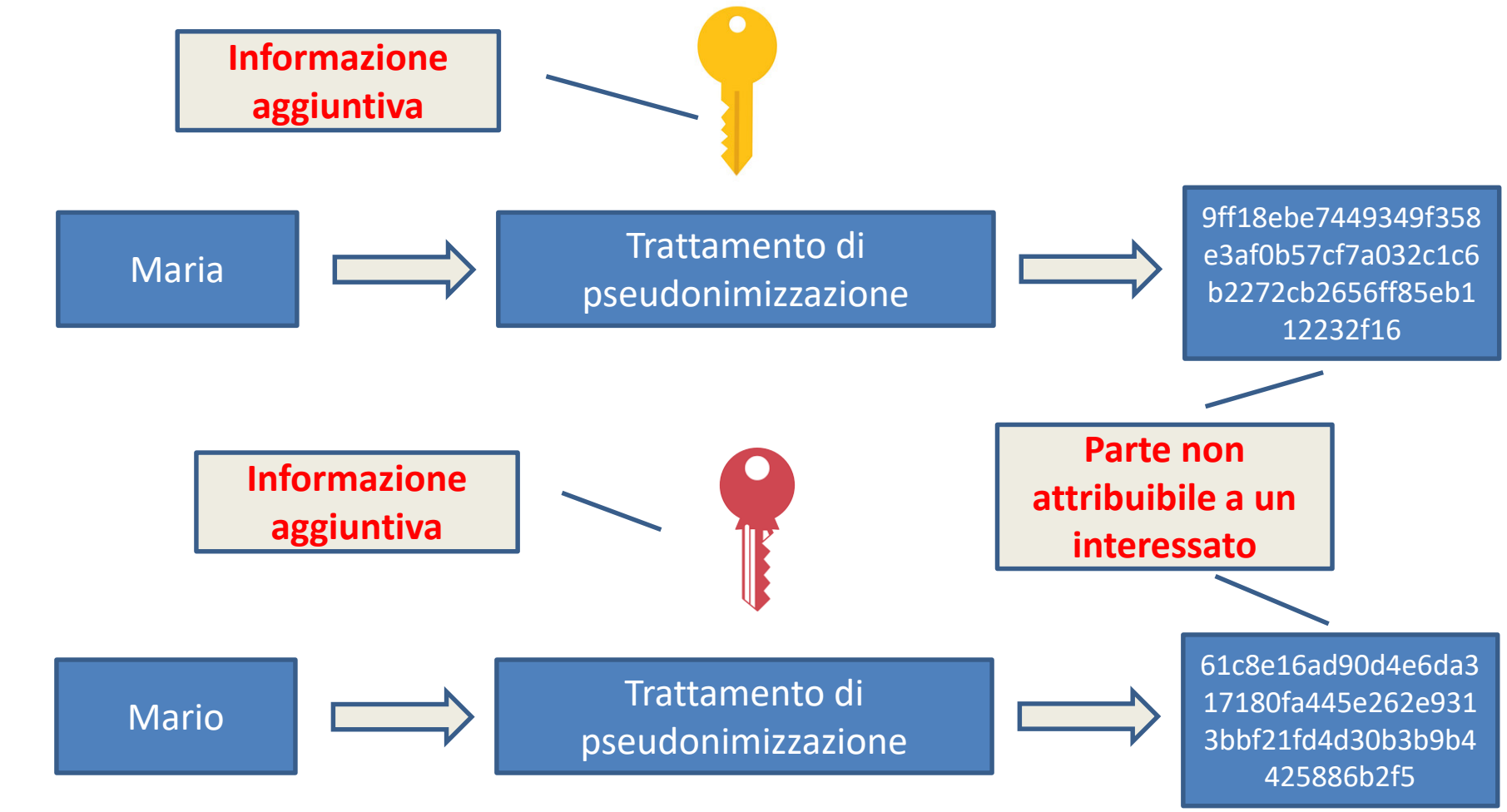
## Attuazione efficace dei principi

- Liceità, correttezza e trasparenza
- Limitazione della finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Pseudonimizzazione in pratica



# Proprietà

- La chiave gira in un solo verso (inversione «computazionalmente» impraticabile)
- Output non intellegibile («quasi» causale)
- Probabilità di collisione trascurabile («praticamente» impossibile)
- Distanza (caratteri diversi) in uscita molto superiore alla distanza (caratteri diversi) in ingresso

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Integrità ed esattezza

| 9ff18ebe7449349f358e3af0b57cf7a032c1c6b2272cb2656ff85eb112232f16 | 9ff18ebe7449349f358e3af0b57cf7a032c1c6b2272cb2656ff85eb112232f16 | 9ff18ebe7449349f358e3af0b57cf7a032c1c6b2272cb2656ff85eb112232f16 | **61c8e16ad90d4e6da317180fa445e262e9313bbf21fd4d30b3b9b4425886b2f5** |
|---|---|---|---|
| Maria | Maria | Maria | Mario |
| t1 | t2 | t3 | tn |

tempo

# Integrità ed esattezza

Local Specialists

24 hour cor care

LA TRAGEDIA

## Vimercate, sacche di sangue scambiate per un caso di omonimia: donna muore in ospedale

È successo a Vimercate. Aperta un'indagine interna. Gli ispettori della Regione al lavoro

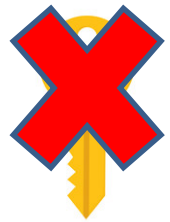
di Simona Ravizza



Il nuovo ospedale di Vimercate disegnato dall'architetto Mario Botta

# Riservatezza

**Distruzione della chiave**



?

Trattamento di pseudonimizzazione

9d1e29cea1a72b63dd ad8504167f028a22fc db994d11fd71beb45a c7d8297474

Chi si nasconde dietro questa identità pseudonimizzata?

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

## La pseudonimizzazione non fa miracoli!

**9d1e29cea1a72b63ddad8504167f028a22fcdb994d11fd71beb45ac7d8297474 ha segnato un gol in rovesciata alla Juventus nel quarto di finale della Champions League 2017-2018**

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# La pseudonimizzazione non fa miracoli!


**Ecco chi è**
**9d1e29cea1a72b63ddad8504167f028a22fcdb9**
**94d11fd71beb45ac7d8297474**

## Minimizzazione

**9d1e29cea1a72b63ddad8504167f028a22fcdb994d11fd71beb45ac7d8297474 ha segnato un gol ~~in rovesciata~~ alla Juventus ~~nel quarto di finale~~ della Champions League 2017-2018**

# Minimizzazione per generalizzazione

| Id | Località | Età | Attributo privato |
|---|---|---|---|
| 1 | 111 | 38 | X |
| 2 | 122 | 39 | X |
| 3 | 122 | 31 | Y |
| 4 | 111 | 33 | Y |
| 5 | 231 | 60 | Z |
| 6 | 231 | 65 | X |
| 7 | 233 | 57 | Y |
| 8 | 233 | 59 | Y |
| 9 | 111 | 41 | Z |
| 10 | 111 | 47 | Z |
| 11 | 122 | 46 | Z |
| 12 | 122 | 45 | Z |

| Id | Località | Età | Attributo privato |
|---|---|---|---|
| 1 | 1* | [30-39] | X |
| 2 | 1* | [30-39] | X |
| 3 | 1* | [30-39] | Y |
| 4 | 1* | [30-39] | Y |
| 5 | 2* | [60-69] | Z |
| 6 | 2* | [60-69] | X |
| 7 | 2* | [50-59] | Y |
| 8 | 2* | [50-59] | Y |
| 9 | 1* | [40-49] | Z |
| 10 | 1* | [40-49] | Z |
| 11 | 1* | [40-49] | Z |
| 12 | 1* | [40-49] | Z |

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Minimizzazione per rotazione delle chiavi

# Correttezza


**Dominio dell'interessato**

**Dominio del titolare**

T4DATA

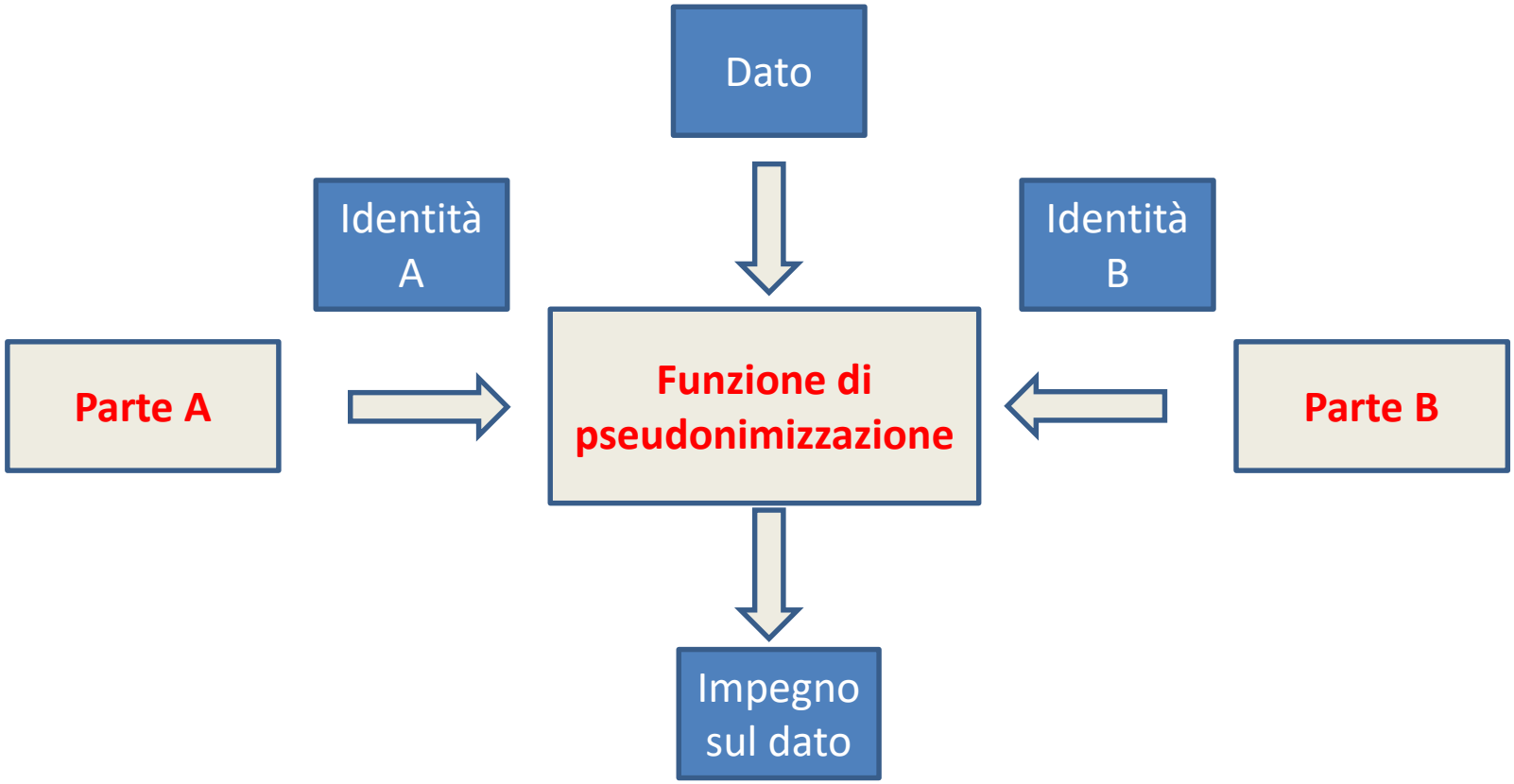
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Art. 11 (Trattamento che non richiede l'identificazione)

1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

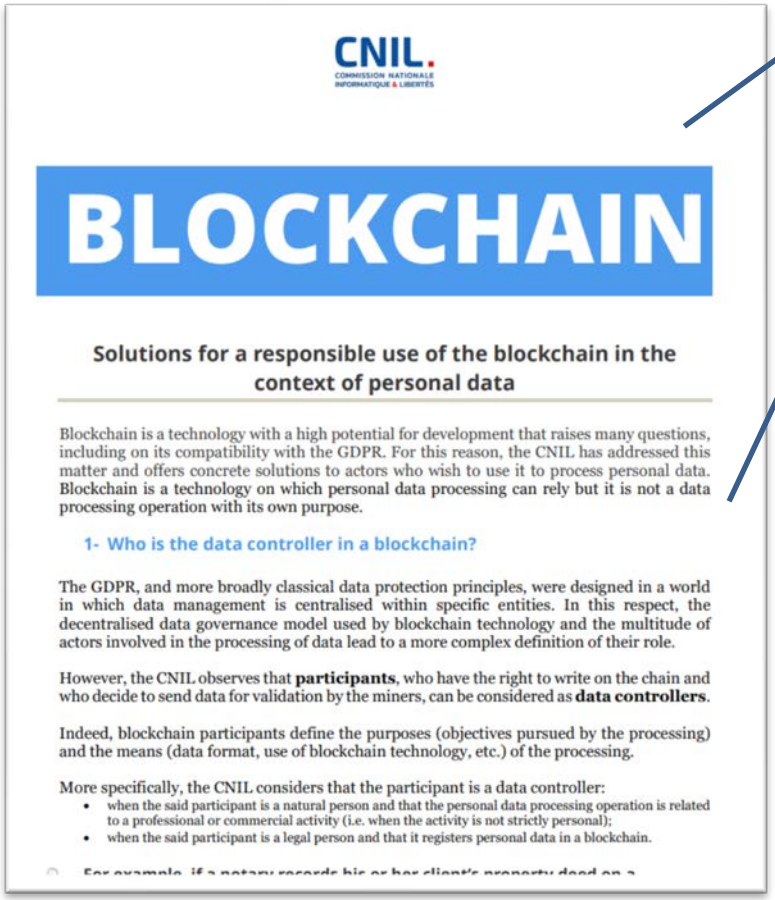
2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

# Limitazione della finalità e della conservazione




Zero knowledge proof (Oded Goldreich, Silvio Micali, Avi Wigderson. Proofs that yield nothing but their validity. Journal of the ACM, volume 38, issue 3, p.690-728. July 1991)

# Limitazione della finalità e della conservazione



CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

**BLOCKCHAIN**

**Solutions for a responsible use of the blockchain in the context of personal data**

Blockchain is a technology with a high potential for development that raises many questions, including on its compatibility with the GDPR. For this reason, the CNIL has addressed this matter and offers concrete solutions to actors who wish to use it to process personal data. Blockchain is a technology on which personal data processing can rely but it is not a data processing operation with its own purpose.

1- Who is the data controller in a blockchain?

The GDPR, and more broadly classical data protection principles, were designed in a world in which data management is centralised within specific entities. In this respect, the decentralised data governance model used by blockchain technology and the multitude of actors involved in the processing of data lead to a more complex definition of their role.

However, the CNIL observes that **participants**, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as **data controllers**.

Indeed, blockchain participants define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing.

More specifically, the CNIL considers that the participant is a data controller:

- when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal);
- when the said participant is a legal person and that it registers personal data in a blockchain.

*…The CNIL considers that personal data should be registered on the blockchain **preferably in the form of a commitment**…*

*…With respect to additional personal data, **in order to ensure compliance with data protection by design** and by default and data minimisation obligations, the CNIL recommends solutions in which data is processed outside of the blockchain or, in which the following are stored on the blockchain, **in order of preference**:*

- *a **commitment** of the data;*
- *a hash generated by a keyed hash function on the data;*
- *a ciphertext of the data.*

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Liceità

**Art. 2-quater (Regole deontologiche)**

**4. Il rispetto delle disposizioni contenute nelle regole deontologiche … costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.**

**Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate (art. 61.1)**

**le misure di garanzia …comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione …(art. 2 septies)**

T4DATA

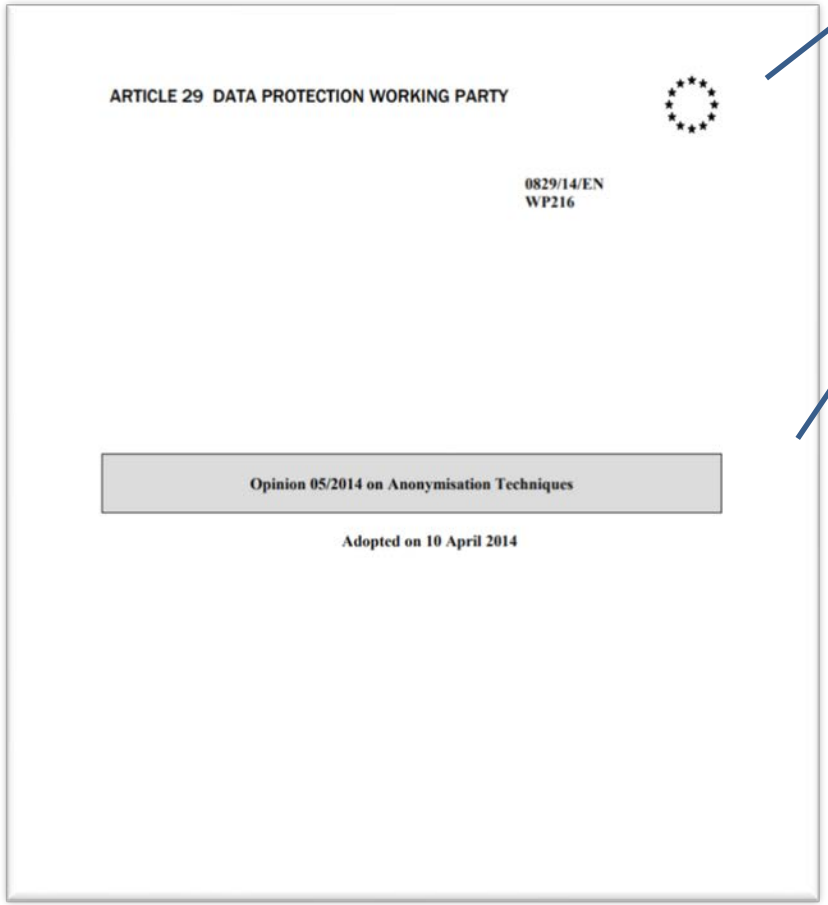
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Anonimizzazione

(26) …. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici…

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Anonimizzazione



ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

*Criteri oggettivi*

- *Single out*
- *Linkability*
- *Inference*

*Aspetti contestuali*

- *Interesse economico del dato*
- *Ampiezza del dataset (o rarità del fenomeno)*
- *Disponibilità di informazione ausiliaria*
- *Idoneità delle misure di sicurezza*
- *Public disclosure*
- *Obblighi contrattuali*

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Conclusioni

Principi e tecnologie

L’opzione «banalizzazione»

L’accountability

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# Grazie

**Giuseppe D’Acquisto**

T4DATA

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# **Accountability e sicurezza dei trattamenti:** misure tecnologiche e responsabilità dei titolari

**Cosimo Comella**
Dipartimento tecnologie digitali e sicurezza informatica

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Agenda

- **Nuovi diritti e nuovi doveri nel trattamento dei dati personali**
- **Il principio di *accountability***
- **Aspetti relativi alla sicurezza dei trattamenti**
- **Valutazione dei rischi**
- **Misure di sicurezza**
- **Nuovo approccio alla sicurezza nel Regolamento europeo**

# La responsabilità dei titolari

**Articolo 24 Responsabilità del titolare del trattamento**

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.[cfr. Art. 28 sui responsabili]

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

# Data protection by default/by design

**Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

# La documentazione dei trattamenti

**Articolo 30 Registri delle attività di trattamento**

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

# La documentazione dei trattamenti

**Articolo 30 Registri delle attività di trattamento (continua)**

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

# La documentazione dei trattamenti

**Articolo 30 Registri delle attività di trattamento (continua)**

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

# Le misure nel Codice previgente erano puntuali

Titolo V - Sicurezza dei dati e dei sistemi

Capo I - Misure di sicurezza

**Art. 31. Obblighi di sicurezza**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Capo II - Misure minime di sicurezza

**Art. 33. Misure minime**

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

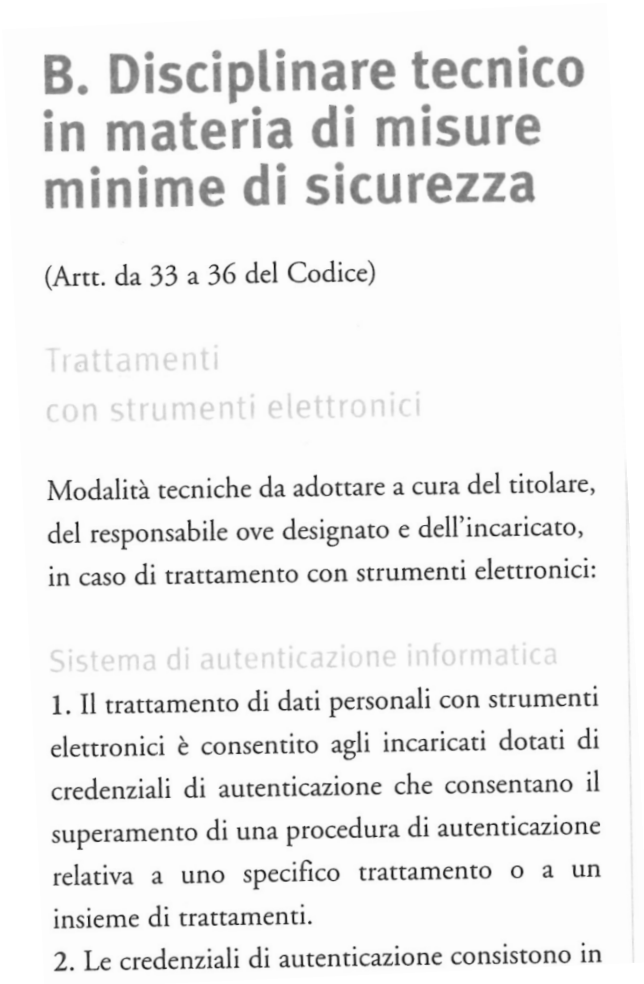
**Art. 34. Trattamenti con strumenti elettronici**

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di

*(testo previgente alle modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101)*

# La sicurezza nel previgente Codice era un elenco di misure puntuali



## B. Disciplinare tecnico in materia di misure minime di sicurezza

(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in

Il Disciplinare tecnico era un manuale operativo, una *check list* di accorgimenti puntuali da adottare per qualunque trattamento

<u>Problemi</u>

- obsolescenza causata dalla veloce evoluzione delle tecnologie e, quindi, delle minacce informatiche
- un set *minimo* è realmente *adeguato* solo ai contesti più semplici
- inattuato aggiornamento delle misure minime ai sensi dell'art. 36 del Codice

*(testo previgente alle modifiche di adeguamento introdotte dal D.Lgs. 10 agosto 2018, n. 101)*

## REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali...

... e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

# La sicurezza informatica nel nuovo Regolamento

*Considerando (39)*

*[…] I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.*

*Considerando (49)*

*Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.*

# La sicurezza informatica nel nuovo Regolamento

*Considerando (71) – decisioni basate su trattamenti automatizzati*

*[…] è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, […]*

Considerando (78)

[…] adottare politiche interne e attuare misure che

- soddisfino in particolare i principi della protezione dei dati fin dalla progettazione *(data protection by design)*
- e della protezione dei dati di come regola sottintesa (*data protection by default)*
- ridurre al minimo il trattamento dei dati personali
- *pseudonimizzare* i dati personali il più presto possibile
- consentire al titolare del trattamento di creare e migliorare le caratteristiche di sicurezza
- i principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici

# La sicurezza informatica nel nuovo Regolamento

*Considerando (81)*

*il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento.*

# La sicurezza informatica nel nuovo Regolamento

*Considerando (83)*

- *Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura.*
- *Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere.*
- *Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*

# La sicurezza informatica nel nuovo Regolamento

*Considerando (89, 90, 91)*

- *trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità*
- *valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*
- *la valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio*
- *valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza.*

# La sicurezza informatica entra a far parte dei princìpi

**REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

*CAPO II*
*Principi*

**Articolo 5**
**Principi applicabili al trattamento di dati personali**

GDPR
GENERAL DATA PROTECTION REGULATION

1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
[...]

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

# Il principio di *responsabilizzazione* o *accountability*

## Article 5. Principles relating to processing of personal data

1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**;
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation')**;
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy')**;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation')**;
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality')**.

# Il principio di *responsabilizzazione* o *accountability*

**Article 5. Principles relating to processing of personal data**

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 **('accountability')**.

- Si tratta della previsione di maggiore impatto su tutto l'impianto del Regolamento.
- Concetto di *accountability* differente da *responsabilità.*
- Difficilmente traducibile mantenendo il senso originale inglese:
- Titolari e Responsabili sono responsabili della *compliance (conformità)* dei trattamenti al GDPR.
- Titolari e responsabili devono essere in grado di dimostrare la conformità al GDPR dei trattamenti in cui sono coinvolti.

# La sicurezza nel GDPR è un insieme di obiettivi

Il GDPR focalizza l'attenzione sugli **obiettivi di sicurezza**

quando?

da perseguire costantemente
cf. *art.32"assicurare su base permanente"*

come?

con misure tecniche e organizzative *adeguate*
cfr. *es. artt. 5, 24, 25, 32*

# Art. 32 – Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
   a) la pseudonimizzazione e la cifratura dei dati personali;
   b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

**art. 24** (1) [...] dette misure sono riesaminate e aggiornate qualora necessario.

# La sicurezza dei trattamenti nel Regolamento europeo

**Art. 32 - Sicurezza del trattamento**

1. Tenendo conto [...] del contesto e delle finalità del trattamento [...] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** [...], che comprendono [...]:

   a)[...]

   b)la capacità di assicurare **su base permanente** la **riservatezza, l'integrità, la disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;

   c)[...]

definizione di "**resilienza**" def. adattata da NIST ([1])

La capacità del sistema informativo di resistere –in una certa misura, tenuto conto delle specificità del trattamento–, a condizioni avverse e di recuperare la normale operatività in maniera sufficientemente rapida da minimizzare la probabilità di incorrere in un danno per gli interessati.


([1]) https://csrc.nist.gov/glossary/term/information-system-resilience

# La sicurezza nel GDPR è un obiettivo...

- Le misure di sicurezza, se *adeguate,* avranno la capacità di assicurare su base permanente gli obiettivi di sicurezza e garantire un livello di protezione costantemente elevato

- L'adeguatezza potrà esser raggiunta solo confezionando tali misure sulle specificità del trattamento. E cioè ...

**Articolo 32**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento...

   ... come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

# La sicurezza nel GDPR è un obiettivo...

**Articolo 32**

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

GDPR
GENERAL DATA PROTECTION REGULATION

# La sicurezza nel GDPR è un obiettivo...

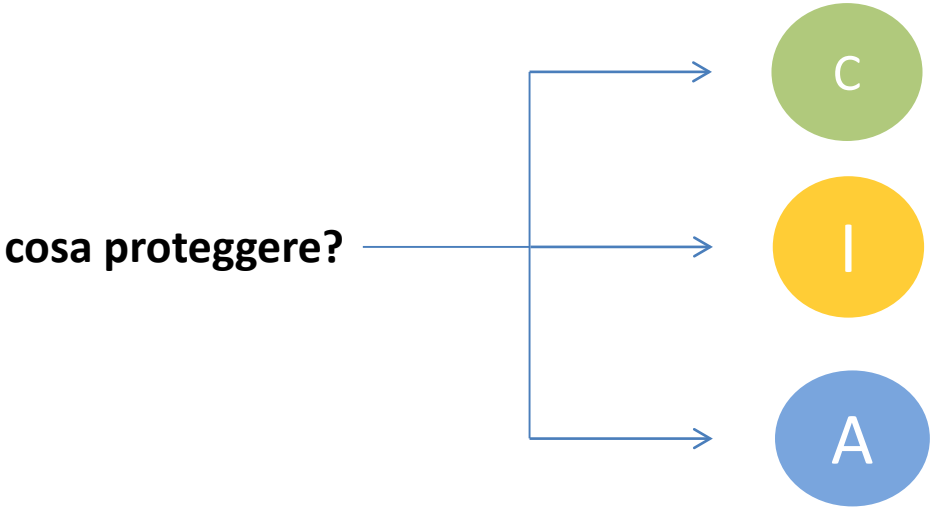
In altri termini, le misure tecniche e organizzative adottate possono essere considerate **adeguate** quando esse sono in grado di assicurare un livello di sicurezza in linea con le risultanze di una valutazione obiettiva e responsabile dei rischi.

I rischi cui fa riferimento il Regolamento sono quelli relativi ai diritti e alle libertà delle persone, correlati allo **specifico** servizio/sistema informativo/attività di *business*, cioè **i rischi che lo specifico trattamento comporta per le persone fisiche cui si riferiscono i dati personali**

**Concetti chiave:**

- adeguatezza delle **misure** tecniche e organizzative
- *specifico* trattamento
- **rischi** per le persone e non per i sistemi informatici
- valutazione dei rischi

# ... la "valutazione dei rischi" è la strada da seguire




**Obiettivi di sicurezza**


**Metodo**

## ... la "valutazione dei rischi" è la strada da seguire

- Il concetto di *valutazione del rischio* è così importante nel Regolamento che il termine **rischio** compare 75 volte nel testo...

# Rischi e misure

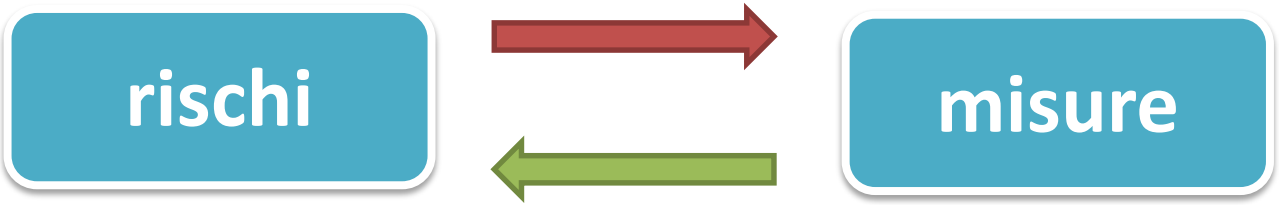

I **rischi** vanno prima **individuati**, poi **valutati**, infine **mitigati** se non **annullati** mediante misure adeguate

Le **misure** vanno **individuate in funzione dei rischi** affinché siano ad essi adeguate e, quindi, **attuate**. Le misure, se adeguate, una volta attuate consentono almeno di mitigare un rischio e, in alcune circostanze, di eliminarlo del tutto.

# Rischi e misure

*la relazione reciproca*

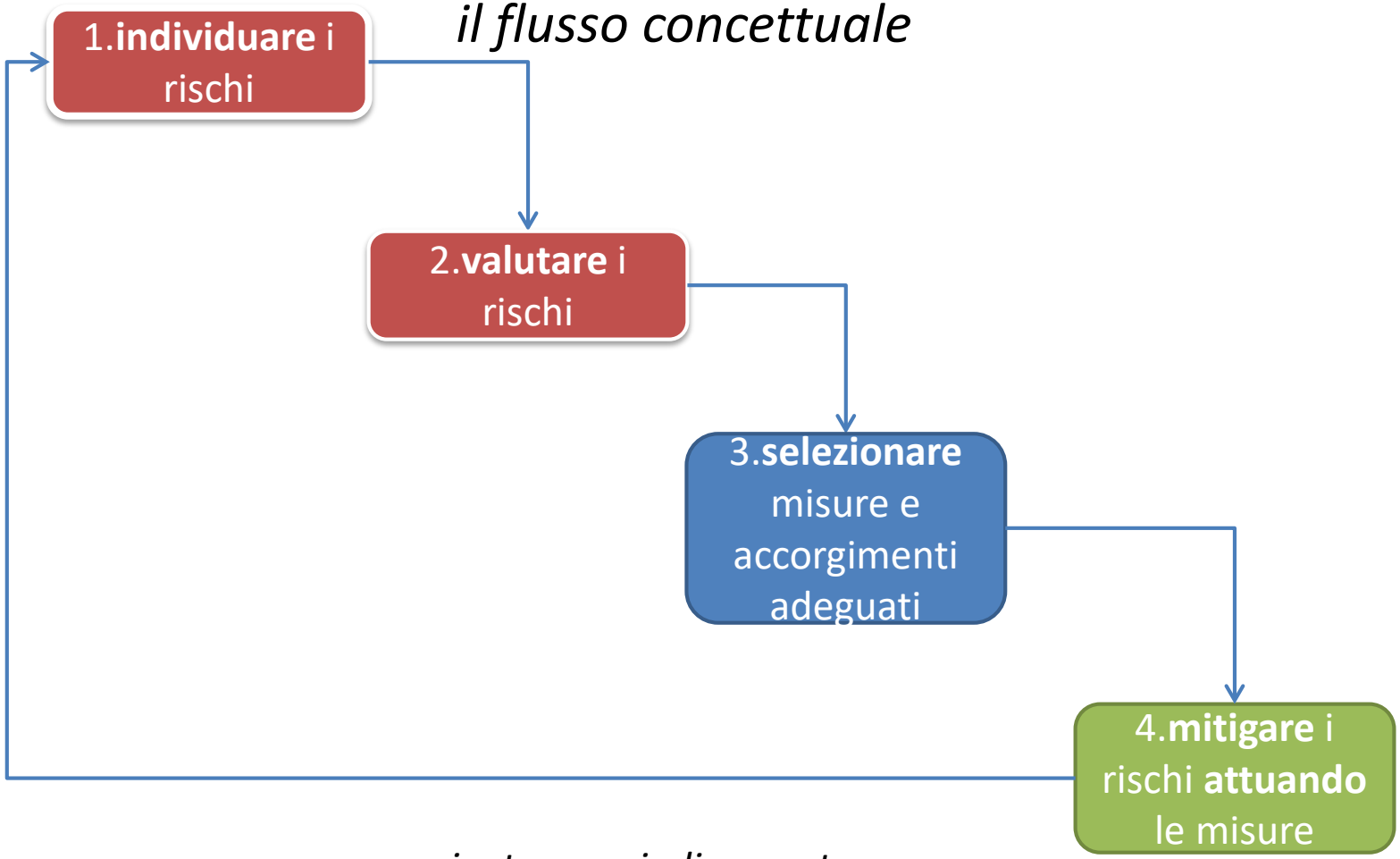
*condizionano la scelta delle*




*servono a mitigare*

# Rischi e misure

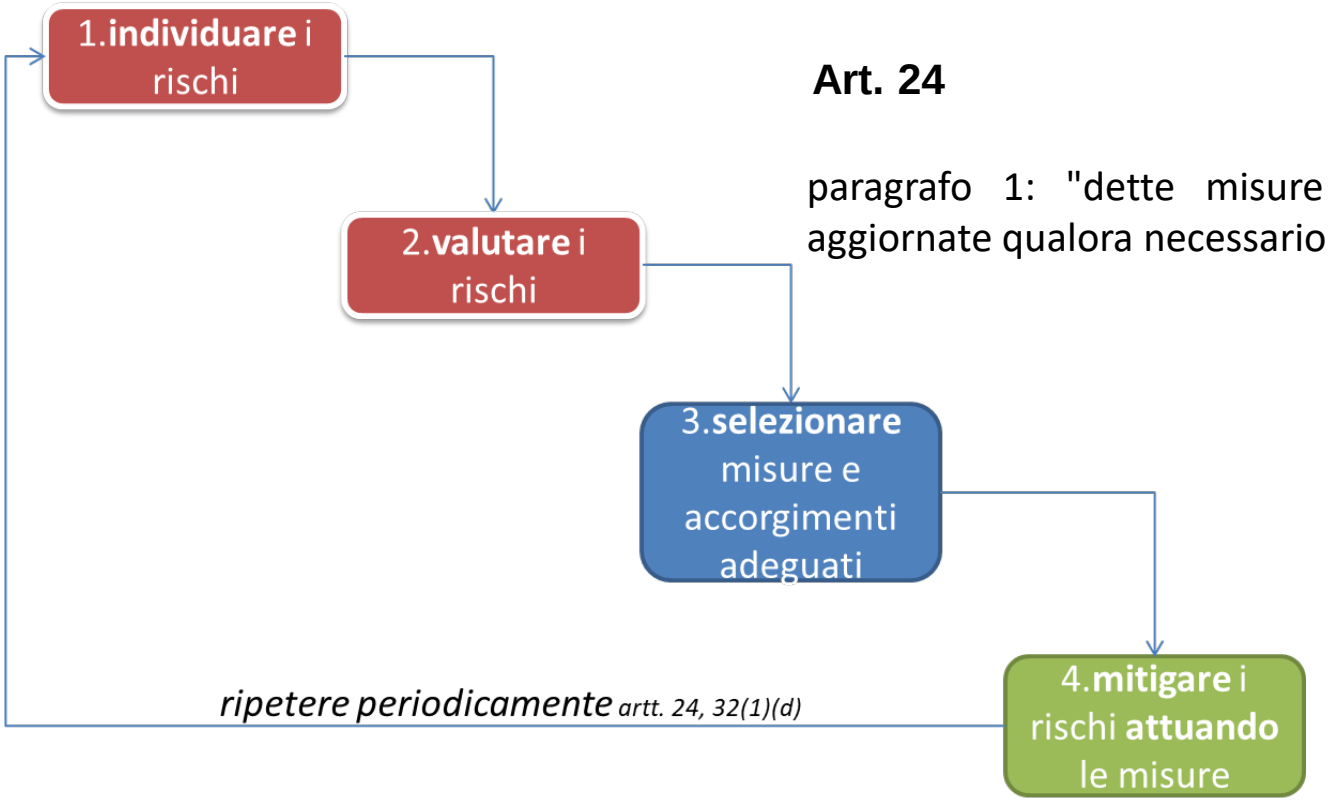
*il flusso concettuale*




*ripetere periodicamente*

*artt. 24, 32(1)(d)*

# Rischi e misure




**Art. 24**

paragrafo 1: "dette misure sono riesaminate e aggiornate qualora necessario"

**Art. 32**

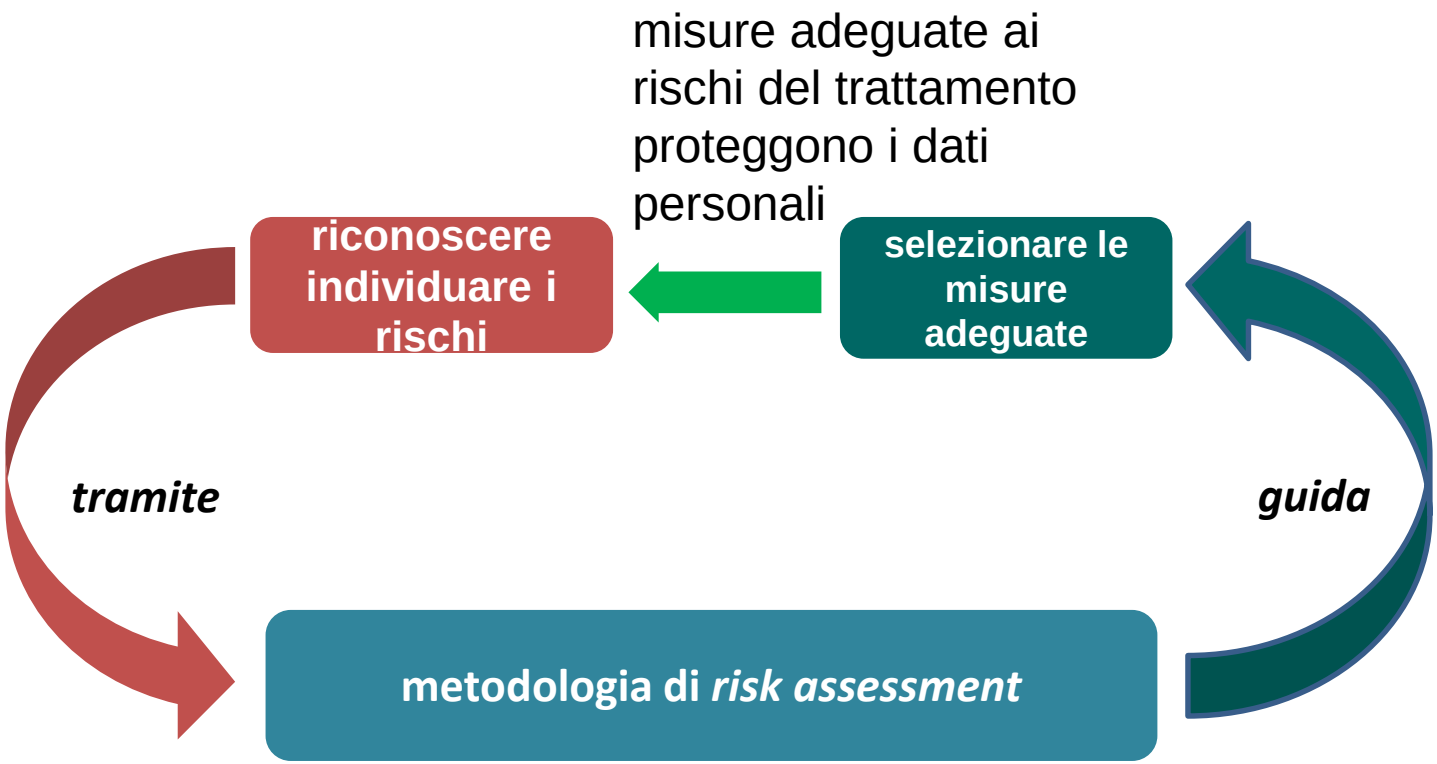
paragrafo 1, lettera d): "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"

## Rischi e misure

La **chiave** per un livello di sicurezza adeguato, consiste nel **riconoscere/individuare** e **valutare** i rischi (dello specifico trattamento) e **selezionare** le **misure adeguate**

***come?***

# Rischi e misure



T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

# Casi pratici di gestione dei data breach: la valutazione del rischio, la notifica al Garante e la comunicazione agli interessati

**Marco Coppotelli**
Dipartimento tecnologie digitali e sicurezza informatica

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Agenda

- **Cos'è un *data breach*?**
- **La gestione di un *data breach***
  - Il rilevamento del *data breach*
  - Il contenimento del *data breach*
  - La valutazione del rischio
  - La notifica del *data breach* al Garante
  - La comunicazione del *data breach* agli interessati
  - La documentazione del *data breach*
- **Il ruolo del responsabile del trattamento**
- **Il ruolo del responsabile della protezione dei dati**
- **Casi pratici di gestione dei *data breach***
- **Dieci regole per la gestione dei *data breach***

# Cos'è un *data breach*? (1)

**Art. 4, punto 12), del Regolamento**

*«**violazione dei dati personali**: 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»*

- Una violazione di sicurezza è un qualsiasi evento che può manifestarsi a seguito di un malfunzionamento *hardware* o *software,* di un attacco informatico o di un comportamento umano doloso o accidentale
- Un *data breach* è una violazione di sicurezza che coinvolge dati personali, in seguito al quale il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali previsti dal Regolamento

# Cos'è un *data breach*? (2)

Un *data breach* può essere classificato
in base ai tre principi della sicurezza delle informazioni

| Violazione della disponibilità | Violazione dell'integrità | Violazione della riservatezza |
|---|---|---|
| *distruzione o perdita non autorizzate di dati personali* | *modifica non autorizzata di dati personali* | *divulgazione o accesso non autorizzati a dati personali* |

Un *data breach* può anche riguardare contemporaneamente
la riservatezza, l'integrità e la disponibilità dei dati personali,
oppure una combinazione delle stesse

# Cos'è un *data breach*? (3)

## Cons. 85 del Regolamento

*«Una **violazione** dei dati personali **può**, se non affrontata in modo adeguato e tempestivo, **provocare danni fisici, materiali o immateriali alle persone fisiche*** […]»


## Possibili conseguenze di un *data breach*

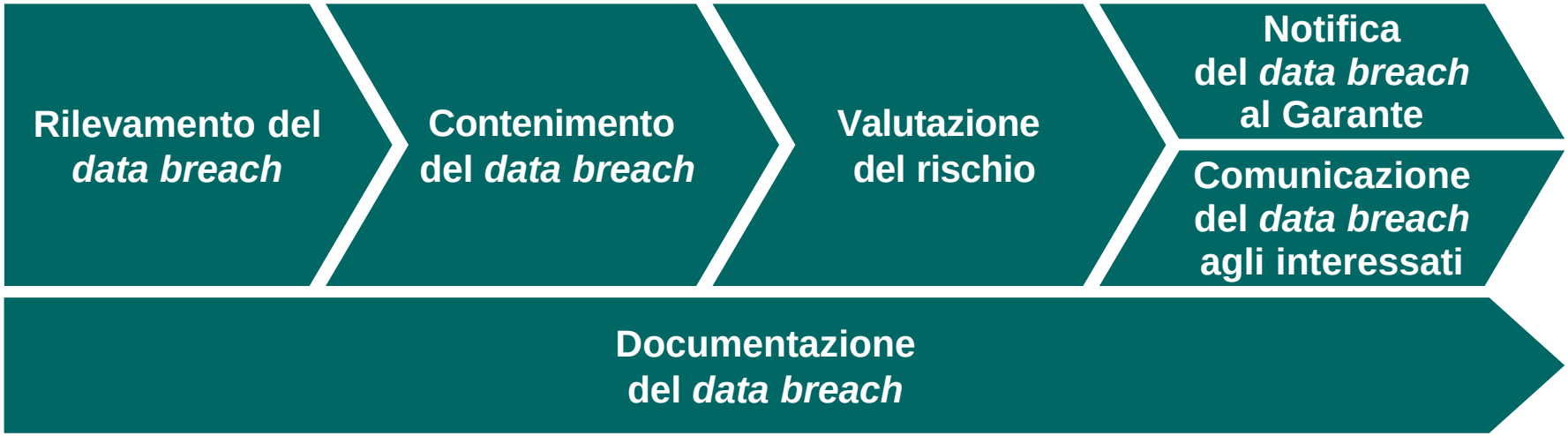
- Perdita di controllo sui dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Pregiudizio alla reputazione
- Decifratura non autorizzata della pseudonimizzazione
- Perdita di riservatezza dei dati protetti da segreto professionale
- Qualsiasi altro danno economico o sociale significativo

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# La gestione di un *data breach*

Il Regolamento stabilisce una serie di adempimenti che un titolare del trattamento è chiamato a compiere a seguito di un *data breach*, anche subordinando i propri interessi economici e di immagine alla tutela dei dati personali degli interessati



# Il rilevamento del *data breach* (1)

**Cons. 87 del Regolamento**

*«È opportuno verificare se siano* ***state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali*** *e informare tempestivamente l'autorità di controllo e l'interessato* […]*»*

Il Regolamento impone ai titolari del trattamento di attuare misure tecniche e organizzative necessarie per rilevare immediatamente un *data breach*, ossia per **assicurarsi di venire "a conoscenza" di un *data breach***

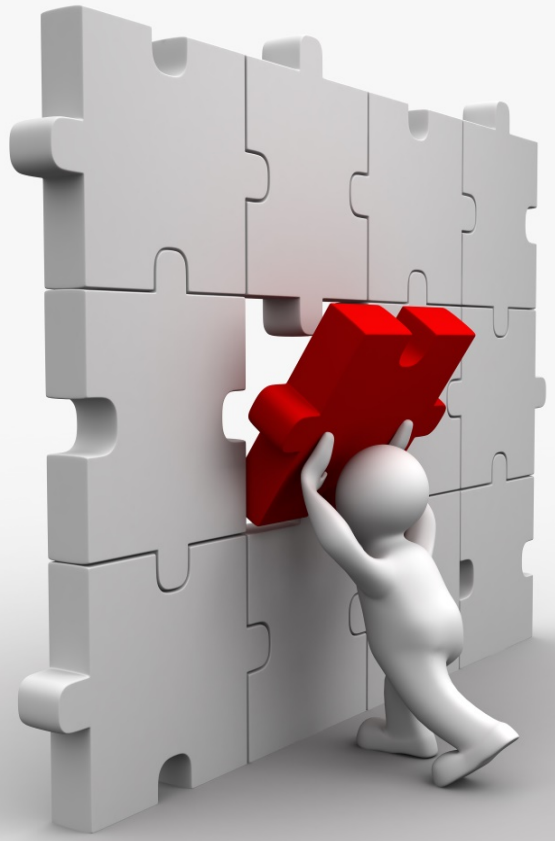
# Il rilevamento del *data breach* (2)

**Cons. 85 del Regolamento**

*«Una violazione dei dati personali può,* ***se non affrontata in modo adeguato e tempestivo****, provocare danni fisici, materiali o immateriali alle persone fisiche* […]»

La capacità di rilevare adeguatamente e tempestivamente un *data breach* è il primo aspetto a cui il titolare del trattamento e il responsabile del trattamento devono rivolgere la loro attenzione

# Il contenimento del *data breach* (1)



- Il titolare del trattamento deve predisporre un **piano di risposta agli incidenti di sicurezza**, che gli consenta di rispondere in maniera efficace e ordinata ai *data breach*
- Il piano di risposta agli incidenti di sicurezza dovrebbe essere documentato e dovrebbe includere una lista di **possibili azioni di mitigazione** e una **chiara assegnazione di ruoli e responsabilità**

# Il contenimento del *data breach* (2)

## Principali azioni di risposta a un *data breach*

- Rimuovere le cause che hanno determinato il *data breach*
- Identificare e mettere in atto misure per attenuare gli effetti negativi del *data breach* per gli interessati
- Ripristinare la normale operatività dei sistemi
- Attivare procedure di *escalation*
- Raccogliere e conservare prove digitali
- Identificare e mettere in atto misure necessarie per evitare che lo stesso *data breach* possa verificarsi di nuovo

# La valutazione del rischio (1)

Gli obblighi di notifica e di comunicazione dei *data breach* introdotti dal Regolamento sono condizionati a una valutazione del rischio effettuata dal titolare del trattamento

- la notifica di un *data breach* al Garante deve essere effettuata "*a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche*" (art. 33, par. 1, del Regolamento)
- la comunicazione di un *data breach* agli interessati è necessaria quando lo stesso "*è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 34, par. 1, del Regolamento)

# La valutazione del rischio (2)

## Cons. 75 del Regolamento

*«I **rischi per i diritti e le libertà delle persone fisiche**, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale*** […]»

## Cons. 76 del Regolamento

*«La **probabilità** e la **gravità** del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla **natura**, all'**ambito di applicazione**, al **contesto** e alle **finalità** del trattamento. Il rischio dovrebbe essere considerato in base a una **valutazione oggettiva** mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato»*

I considerando 75 e 76 del Regolamento suggeriscono di valutare il rischio in modo oggettivo, tenendo conto tanto della **probabilità** quanto della **gravità del rischio per i diritti e le libertà delle persone fisiche**

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# La valutazione del rischio (3)

## Fattori da considerare nella valutazione del rischio

Le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679*" (WP250 rev.01) individuano alcuni dei fattori da considerare nella valutazione del rischio

Scan me


- **Tipo di violazione**
- **Natura, carattere sensibile e volume dei dati personali**
- **Numero di persone fisiche interessate**
- **Facilità di identificazione delle persone fisiche**
- **Gravità delle conseguenze per le persone fisiche**
- **Caratteristiche particolari dell'interessato**
- **Caratteristiche particolari del titolare del trattamento**

# La valutazione del rischio (4)

**È PROBABILE CHE CI SIA UN RISCHIO ELEVATO**

- Contenimento del *data breach*
- Notifica al Garante
- Comunicazione agli interessati
- Documentazione del *data breach*

**È PROBABILE CHE CI SIA UN RISCHIO**

- Contenimento del *data breach*
- Notifica al Garante
- Documentazione del *data breach*

**È IMPROBABILE CHE CI SIA UN RISCHIO**

- Contenimento del *data breach*
- Documentazione del *data breach*

# La notifica del *data breach* al Garante (1)

**Art. 33, par. 1, del Regolamento**

*«In caso di violazione dei dati personali, **il titolare del trattamento notifica la violazione all'autorità di controllo** competente a norma dell'articolo 55 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei **motivi del ritardo**»*

# La notifica del *data breach* al Garante (2)

## Contenuto della notifica al Garante

**Art. 33, par. 3, del Regolamento**

*«La notifica di cui al paragrafo 1 deve almeno:*

*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**»*

# La notifica del *data breach* al Garante (3)

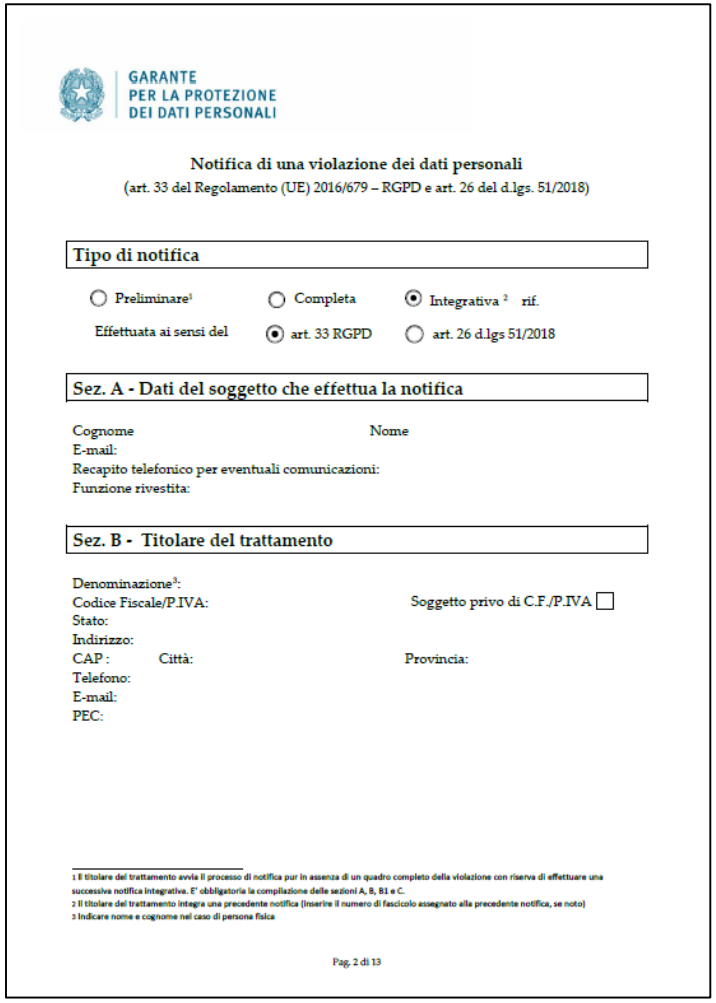
## Contenuto della notifica al Garante

Con il Provvedimento n. 157 del 30 luglio 2019, il Garante ha indicato le informazioni da fornire, in caso di *data breach*, nella notifica prevista dall'art. 33 del Regolamento


Scan me

Notifica da sottoscrivere con firma digitale o con firma autografa e da trasmettere all'indirizzo protocollo@pec.gpdp.it

# La notifica del *data breach* al Garante (4)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Notifica di una violazione dei dati personali**
(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

**Tipo di notifica**

○ Preliminare[1] ○ Completa ◉ Integrativa[2] rif.
Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

**Sez. A - Dati del soggetto che effettua la notifica**

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

**Sez. B - Titolare del trattamento**

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP: Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (Inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

Pag. 2 di 13

## Contenuto della notifica

**Tipo di notifica**

- Preliminare, Completa o Integrativa
- art. 33 GDPR o art. 26 d.lgs. 51/2008

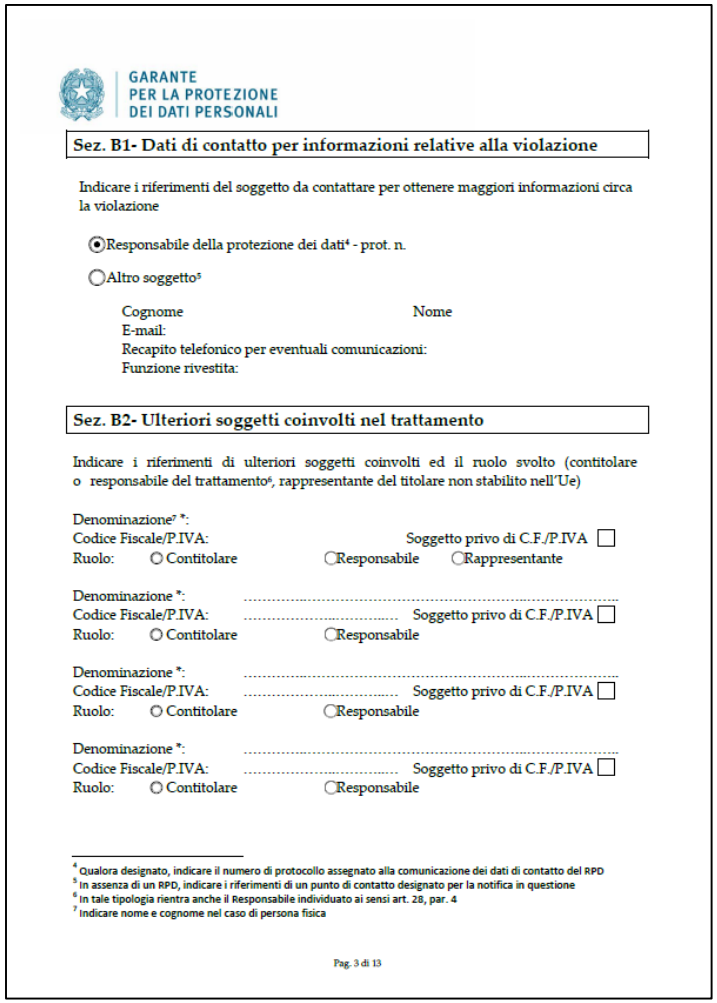
**Sez. A - Dati del soggetto che effettua la notifica**

- Cognome
- Nome
- Dati di contatto

**Sez. B - Titolare del trattamento**

- Denominazione
- Codice fiscale o Partita IVA
- Dati di contatto

# La notifica del *data breach* al Garante (5)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. B1- Dati di contatto per informazioni relative alla violazione**

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

**Sez. B2- Ulteriori soggetti coinvolti nel trattamento**

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: .....
Codice Fiscale/P.IVA: ..... Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Pag. 3 di 13

## Contenuto della notifica

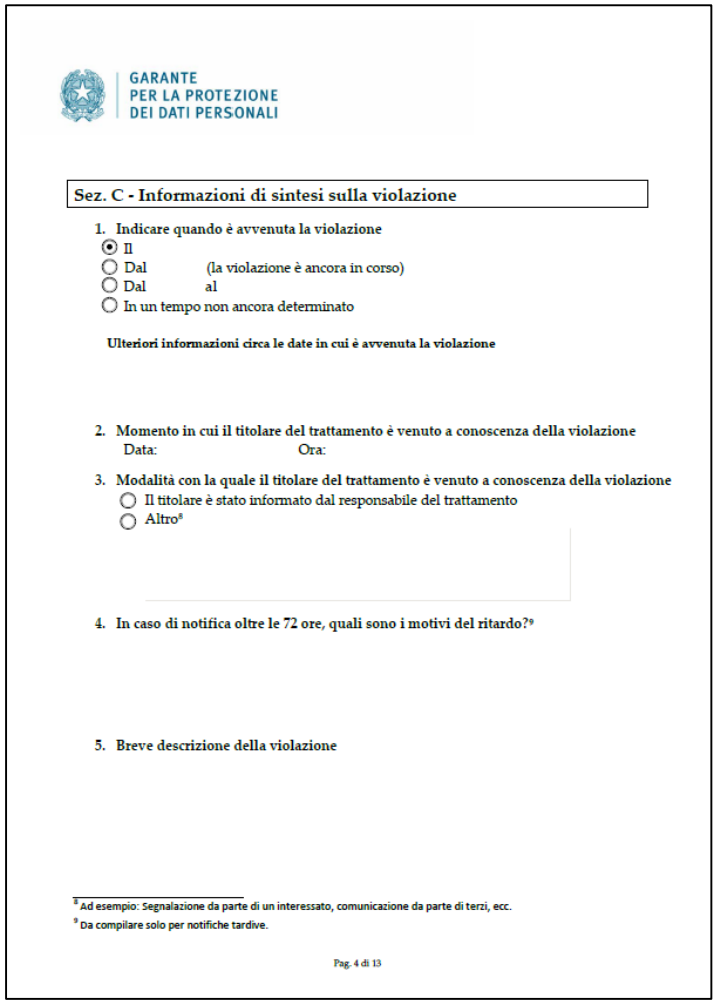
**Sez. B1 - Dati di contatto per ottenere più informazioni sul *data breach***

- Responsabile della protezione dei dati
- Altro soggetto

**Sez. B2 - Ulteriori soggetti coinvolti**

- Contitolari del trattamento
- Responsabili del trattamento
- Rappresentante del titolare non stabilito nell'UE

# La notifica del *data breach* al Garante (6)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. C - Informazioni di sintesi sulla violazione**

1. Indicare quando è avvenuta la violazione
   - (•) Il
   - ( ) Dal (la violazione è ancora in corso)
   - ( ) Dal al
   - ( ) In un tempo non ancora determinato

   **Ulteriori informazioni circa le date in cui è avvenuta la violazione**

2. Momento in cui il titolare del trattamento è venuto a conoscenza della violazione
   Data: Ora:
3. Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione
   - ( ) Il titolare è stato informato dal responsabile del trattamento
   - ( ) Altro[8]
4. In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]
5. Breve descrizione della violazione

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.
[9] Da compilare solo per notifiche tardive.

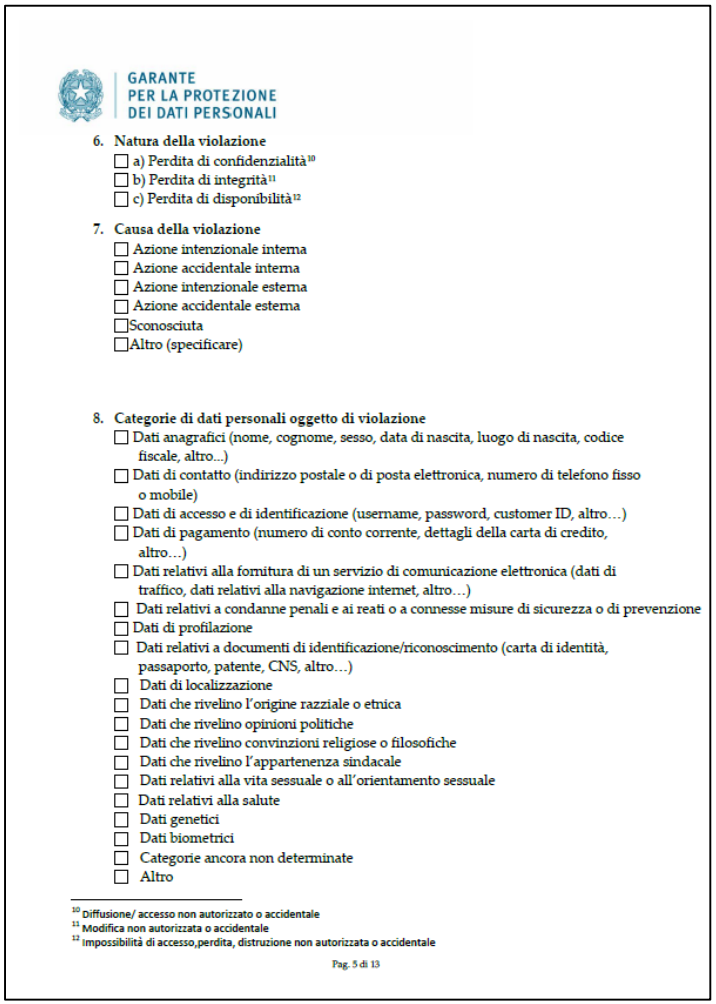
Pag. 4 di 13

## Contenuto della notifica

**Sez. C - Informazioni di sintesi sul *data breach***

- Periodo in cui è avvenuta la violazione
- Momento in cui il titolare è venuto "a conoscenza" della violazione
- Modalità con la quale il titolare è venuto "a conoscenza" della violazione
- Motivi dell'eventuale ritardo nella notifica al Garante
- Breve descrizione della violazione

# La notifica del *data breach* al Garante (7)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

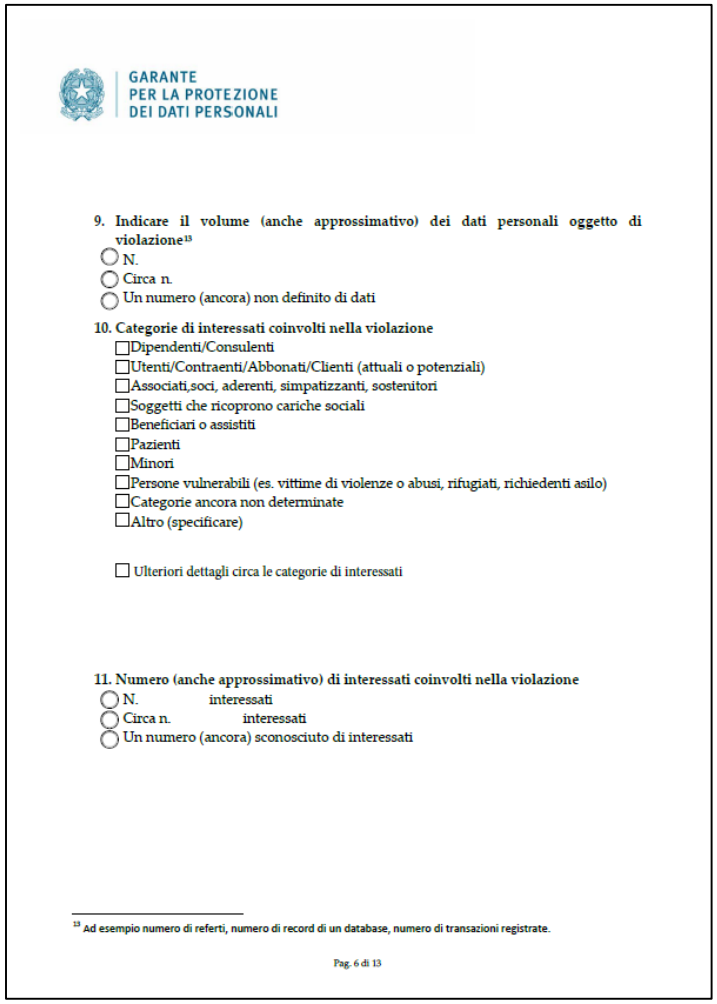
Pag. 5 di 13

## Contenuto della notifica

**Sez. C - Informazioni di sintesi sul *data breach***

- Natura della violazione
  - perdita di confidenzialità
  - perdita di integrità
  - perdita di disponibilità
- Causa della violazione
  - azione interna/esterna
  - azione intenzionale/accidentale
- Categorie di dati personali oggetto di violazione
  - dati anagrafici, di contatto, di accesso, di pagamento
  - dati di categorie particolari (art. 9 GDPR)
  - dati relativi a condanne penali e reati (art. 10 GDPR)

# La notifica del *data breach* al Garante (8)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]
- ◯ N.
- ◯ Circa n.
- ◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione
- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione
- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

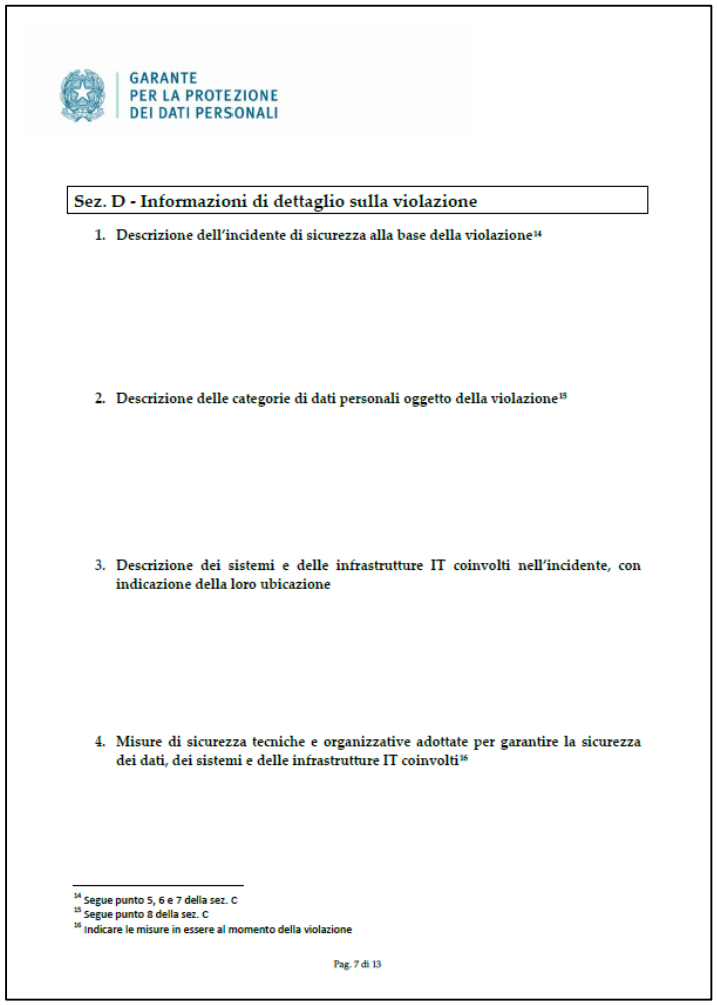
Pag. 6 di 13

## Contenuto della notifica

**Sez. C - Informazioni di sintesi sul *data breach***

- Volume dei dati personali oggetto di violazione
- Categorie di interessati coinvolti nella violazione
  - dipendenti
  - utenti/contraenti/abbonati/clienti
  - pazienti
  - minori
  - ecc.
- Numero di interessati coinvolti nella violazione

# La notifica del *data breach* al Garante (9)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. D - Informazioni di dettaglio sulla violazione**

1. Descrizione dell'incidente di sicurezza alla base della violazione[14]

2. Descrizione delle categorie di dati personali oggetto della violazione[15]

3. Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione

4. Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

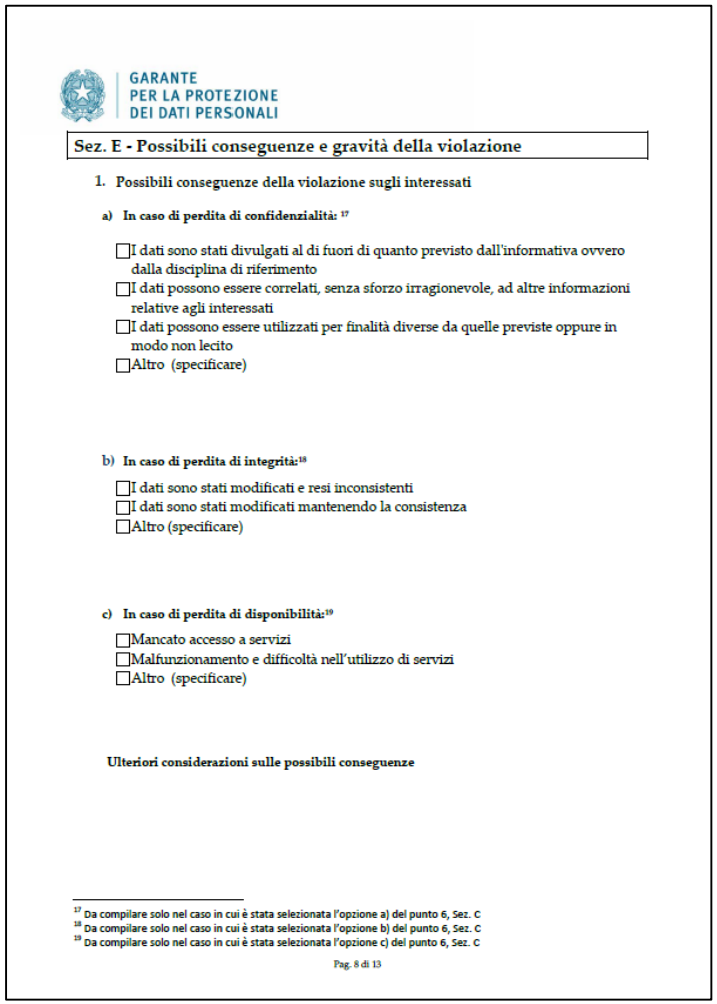
Pag. 7 di 13

## Contenuto della notifica

**Sez. D - Informazioni di dettaglio sul *data breach***

- Descrizione dell'incidente di sicurezza che ha determinato la violazione
- Descrizione delle categorie di dati personali oggetto di violazione
- Descrizione dei sistemi e delle infrastrutture IT coinvolti nella violazione
- Misure di sicurezza adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti

# La notifica del *data breach* al Garante (10)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. E - Possibili conseguenze e gravità della violazione**

1. **Possibili conseguenze della violazione sugli interessati**

**a) In caso di perdita di confidenzialità: [17]**

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

**b) In caso di perdita di integrità: [18]**

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

**c) In caso di perdita di disponibilità: [19]**

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

**Ulteriori considerazioni sulle possibili conseguenze**

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

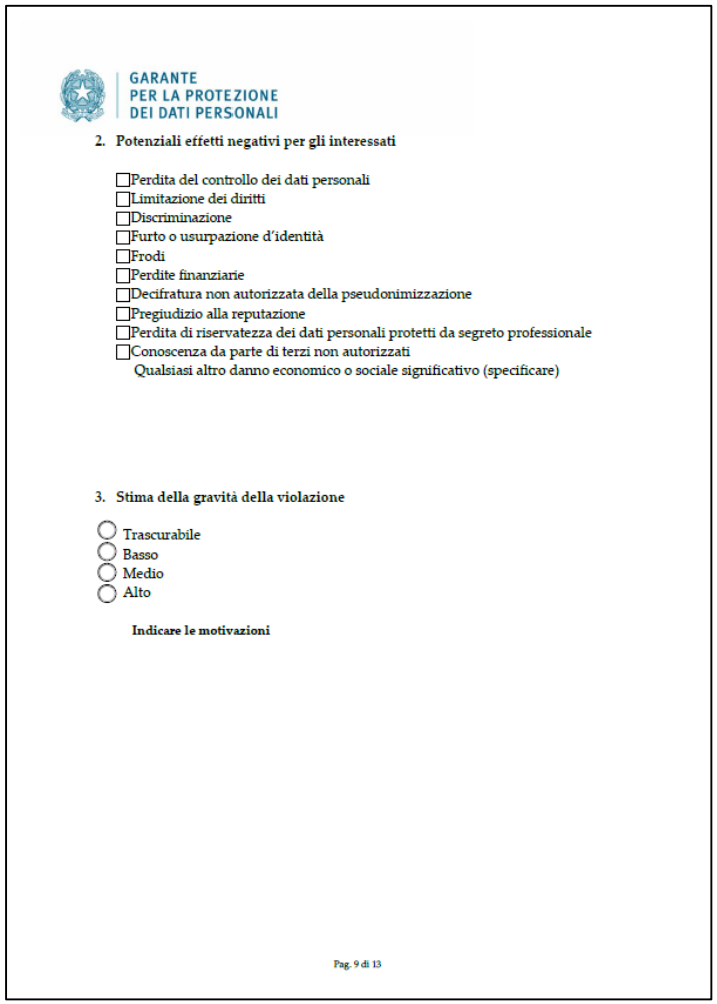
Pag. 8 di 13

## Contenuto della notifica

**Sez. E - Conseguenze e gravità del *data breach***

- Possibili conseguenze del *data breach*
  - in caso di perdita della confidenzialità
  - in caso di perdita dell'integrità
  - in caso di perdita della disponibilità

# La notifica del *data breach* al Garante (11)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

2. **Potenziali effetti negativi per gli interessati**

- ☐ Perdita del controllo dei dati personali
- ☐ Limitazione dei diritti
- ☐ Discriminazione
- ☐ Furto o usurpazione d'identità
- ☐ Frodi
- ☐ Perdite finanziarie
- ☐ Decifratura non autorizzata della pseudonimizzazione
- ☐ Pregiudizio alla reputazione
- ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
- ☐ Conoscenza da parte di terzi non autorizzati

Qualsiasi altro danno economico o sociale significativo (specificare)

3. **Stima della gravità della violazione**

- ◯ Trascurabile
- ◯ Basso
- ◯ Medio
- ◯ Alto

**Indicare le motivazioni**

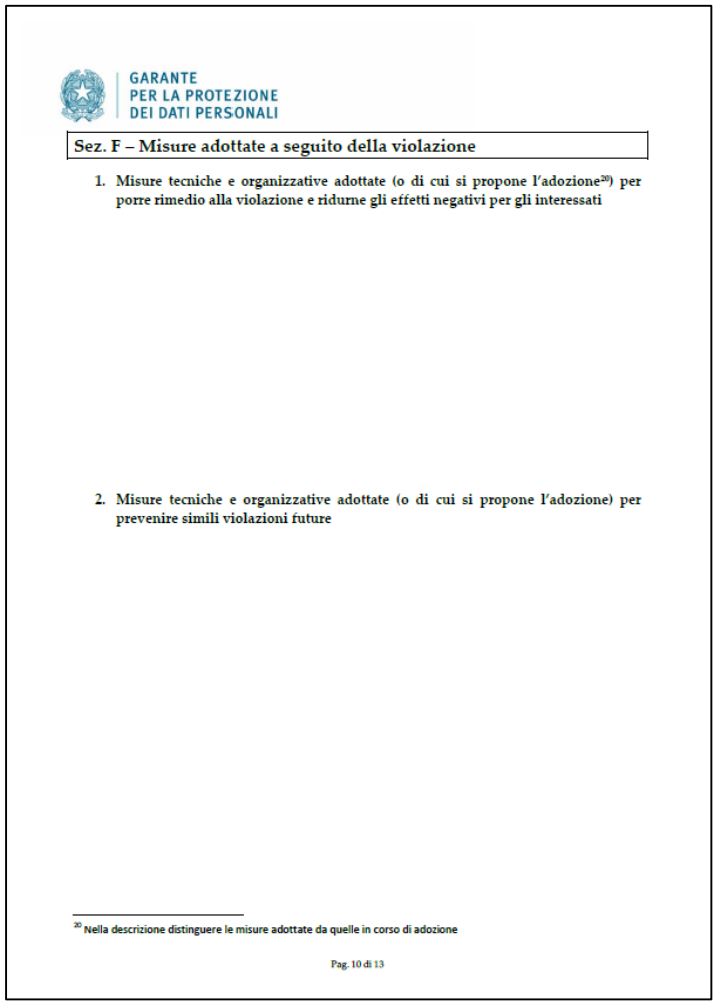
Pag. 9 di 13

## Contenuto della notifica

**Sez. E - Conseguenze e gravità del *data breach***

- Possibili effetti negativi per gli interessati
  - perdita del controllo dei dati personali
  - limitazione dei diritti
  - discriminazione
  - ecc.
- Stima della gravità della violazione
  - trascurabile
  - bassa
  - media
  - alta

# La notifica del *data breach* al Garante (12)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. F – Misure adottate a seguito della violazione**

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

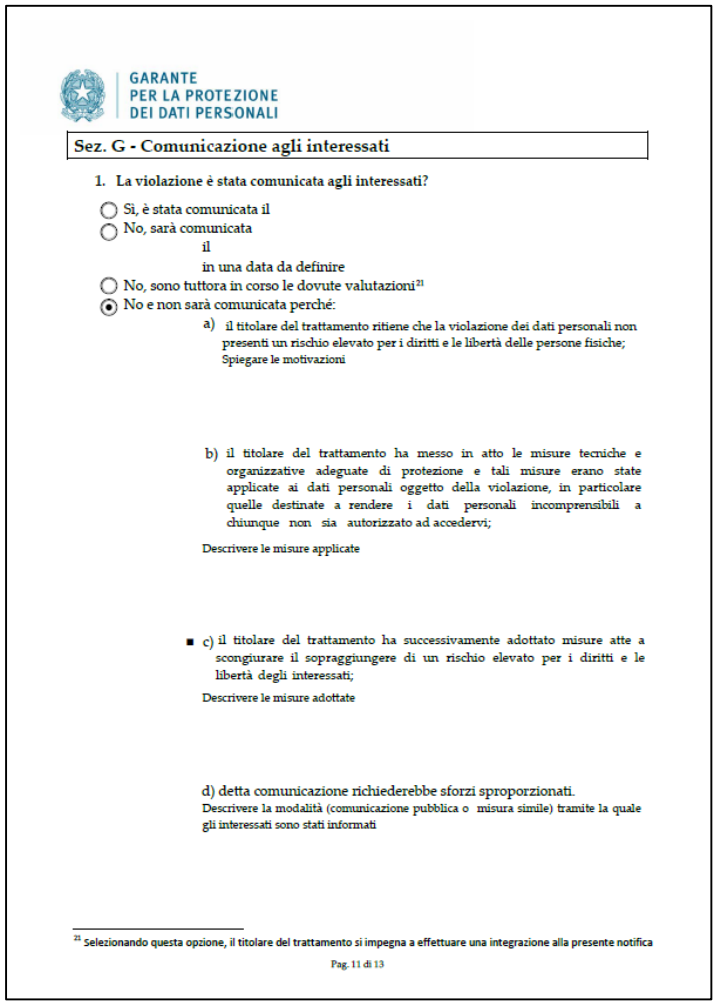
Pag. 10 di 13

## Contenuto della notifica

**Sez. F - Misure adottate a seguito del *data breach***

- Misure tecniche e organizzative adottate, o che si intende adottare, per porre rimedio al *data breach* e ridurre gli effetti negativi per gli interessati
- Misure tecniche e organizzative adottate, o che si intende adottare, per prevenire simili violazioni future

# La notifica del *data breach* al Garante (13)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. G - Comunicazione agli interessati**

1. **La violazione è stata comunicata agli interessati?**

◯ Sì, è stata comunicata il
◯ No, sarà comunicata il
in una data da definire
◯ No, sono tuttora in corso le dovute valutazioni[21]
◉ No e non sarà comunicata perché:

a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche; Spiegare le motivazioni

b) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;

Descrivere le misure applicate

■ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

d) detta comunicazione richiederebbe sforzi sproporzionati.
Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

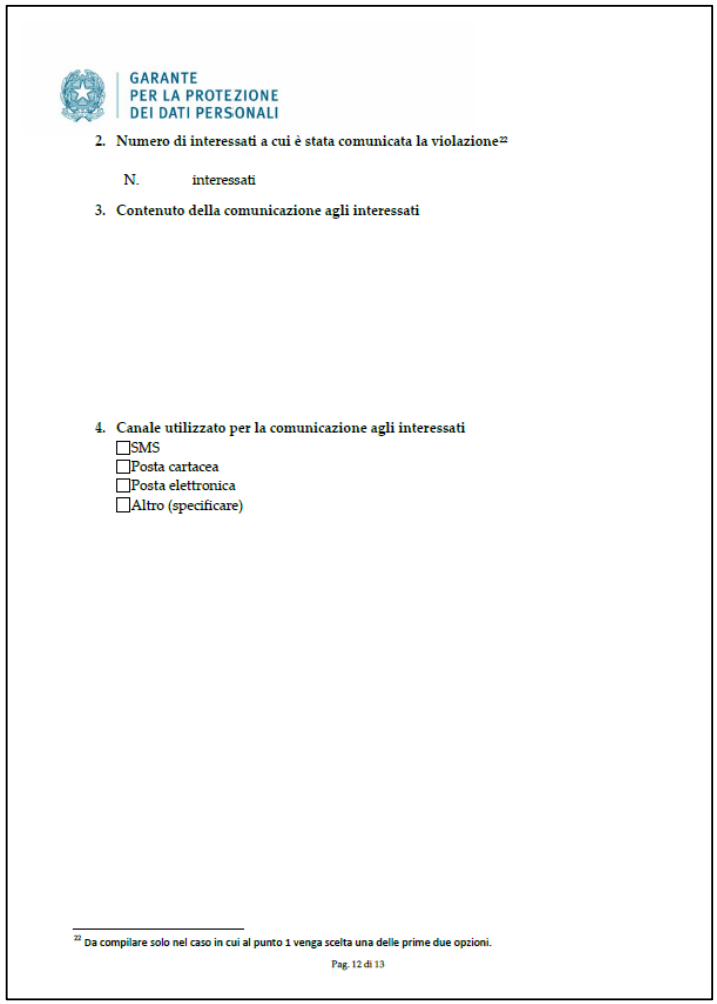
Pag. 11 di 13

## Contenuto della notifica

**Sez. G - Comunicazione agli interessati**

- Violazione comunicata agli interessati?
  - Sì, è stata comunicata il …
  - No, sarà comunicata il …
  - No, sono tuttora in corso le dovute valutazioni
  - No, non è stata comunicata perché …

# La notifica del *data breach* al Garante (14)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

2. Numero di interessati a cui è stata comunicata la violazione[22]

N. interessati

3. Contenuto della comunicazione agli interessati

4. Canale utilizzato per la comunicazione agli interessati
☐SMS
☐Posta cartacea
☐Posta elettronica
☐Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

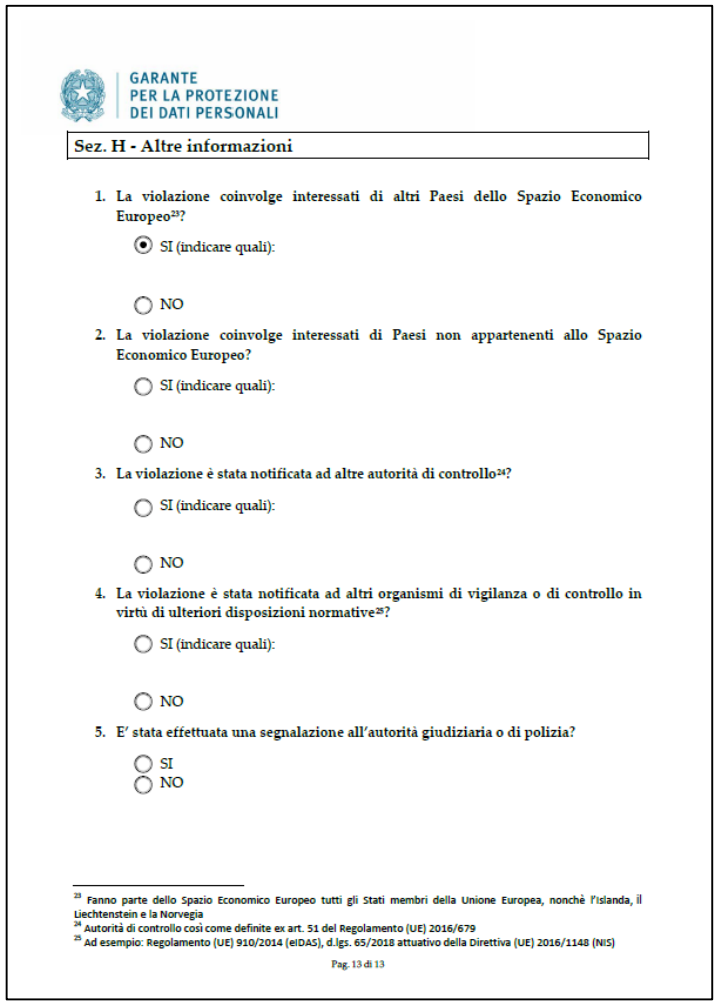
Pag. 12 di 13

## Contenuto della notifica

**Sez. G - Comunicazione agli interessati**

- Numero di interessati a cui è stato comunicato il *data breach*
- Contenuto della comunicazione
- Canale utilizzato per la comunicazione
  - SMS
  - Posta ordinaria
  - Posta elettronica
  - Altro

# La notifica del *data breach* al Garante (15)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**Sez. H - Altre informazioni**

1. La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?
   - (•) SI (indicare quali):
   - ( ) NO
2. La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?
   - ( ) SI (indicare quali):
   - ( ) NO
3. La violazione è stata notificata ad altre autorità di controllo[24]?
   - ( ) SI (indicare quali):
   - ( ) NO
4. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?
   - ( ) SI (indicare quali):
   - ( ) NO
5. E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?
   - ( ) SI
   - ( ) NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

Pag. 13 di 13

## Contenuto della notifica

**Sez. H - Altre informazioni**

- *Data breach* coinvolge interessati residenti in altri Paesi dello Spazio Economico Europeo?
- *Data breach* coinvolge interessati residenti in Paesi fuori dallo Spazio Economico Europeo?
- *Data breach* notificato ad altre autorità di controllo?
- *Data breach* notificato ad altri organismi di vigilanza o di controllo?
- Segnalazione all'autorità giudiziaria?

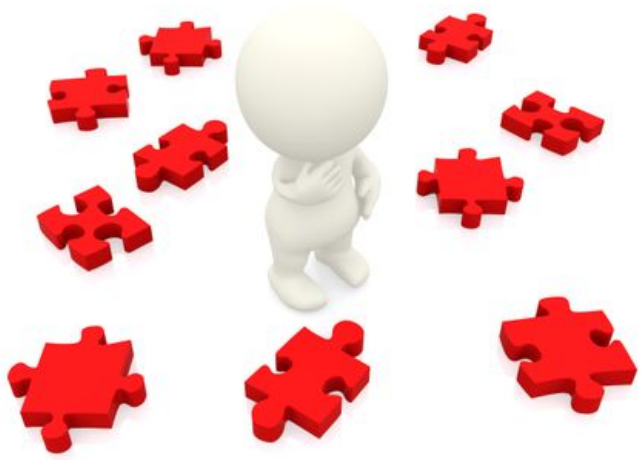
# La notifica del *data breach* al Garante (16)

## Notifica di un *data breach* per fasi

Un titolare del trattamento potrebbe non disporre di tutte le informazioni relative a un *data breach* entro 72 ore dal momento in cui ne è venuto a conoscenza

**Art. 33, par. 4, del Regolamento**

*«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»*



# La comunicazione del *data breach* agli interessati (1)

## Art. 34, par. 1, del Regolamento

*«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**»*

## Cons. 86 del Regolamento

*«Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, **al fine di consentirgli di prendere le precauzioni necessarie.***
[…] *Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva»*

# La comunicazione del *data breach* agli interessati (2)

**Art. 34, par. 2, del Regolamento**

*«La comunicazione all'interessato di cui al paragrafo 1 del presente articolo 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)»*

**Cons. 86 del Regolamento**

«[…] *La comunicazione dovrebbe* ***descrivere la natura della violazione*** *dei dati personali e* ***formulare raccomandazioni*** *per la persona fisica interessata* ***intese ad attenuare i potenziali effetti negativi*** […]»

## Contenuto della comunicazione

- Descrizione della natura del *data breach*
- Punto di contatto (DPO o altro soggetto)
- Possibili conseguenze della violazione
- Misure adottate, o che si intende adottare, per porre rimedio al *data breach*
- Misure adottate, o che si intende adottare, per attenuare gli effetti negativi del *data breach* per gli interessati
- Indicazioni pratiche sulle misure che gli interessati possono adottare per proteggersi da conseguenze negative

# La comunicazione del *data breach* agli interessati (3)

L'**obiettivo principale** della comunicazione agli interessati consiste nel fornire loro **informazioni specifiche sulle misure che questi possono prendere per proteggersi**

Il titolare del trattamento:

- deve individuare il canale di contatto più appropriato per comunicare una violazione agli interessati
- può utilizzare diversi canali di contatto, anziché un singolo canale
- deve essere cauto nell'usare un canale di contatto compromesso dalla violazione

# La comunicazione del *data breach* agli interessati (4)

## Casi in cui non va effettuata la comunicazione

**Art. 34, par. 3, del Regolamento**

*«Non è richiesta la comunicazione all'interessato* […] *se è soddisfatta una delle seguenti condizioni:*

a) *il titolare del trattamento* ***ha messo in atto le misure tecniche e organizzative*** *adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle* ***destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi****, quali la cifratura;*

b) *il titolare del trattamento* ***ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato*** *per i diritti e le libertà degli interessati di cui al paragrafo 1;*

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»*

# La documentazione del *data breach* (1)

**Art. 33, par. 5, del Regolamento**

*«Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo»*

## Contenuto minimo della documentazione

- Dettagli relativi al *data breach*, comprese le cause, il numero e le categorie di interessati, il numero e le categorie di dati personali
- Effetti e conseguenze del *data breach*
- Ragionamenti alla base delle decisioni prese in risposta al *data breach*

# La documentazione del *data breach* (2)

Il titolare del trattamento dovrebbe:

- documentare i motivi per i quali ha ritenuto di non dover notificare un *data breach*
- documentare le decisioni e le misure adottate per porre rimedio a un *data breach*
- documentare i motivi dell'eventuale ritardo nella notifica al Garante di un *data breach*
- documentare la ricorrenza di una delle condizioni per cui non è necessaria la comunicazione agli interessati
- conservare elementi utili a dimostrare l'avvenuta comunicazione agli interessati

# Il ruolo del responsabile della protezione dei dati (1)

## Art. 39 del Regolamento

*«Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:*

*a)* ***informare e fornire consulenza al titolare del trattamento*** […]

*b)* ***sorvegliare l'osservanza del presente regolamento****,* […]

*d)* ***cooperare con l'autorità di controllo****; e*

*e)* ***fungere da punto di contatto per l'autorità di controllo*** *per questioni connesse al trattamento,* […]»

## Art. 33, par. 3, del Regolamento

*«La notifica di cui al paragrafo 1 deve almeno:* […]

*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;* […]»

# Il ruolo del responsabile della protezione dei dati (2)

Le "*Linee guida sulla notifica delle violazioni dei dati personali*" indicano alcuni compiti che potrebbero essere assegnati al responsabile della protezione dei dati

Il responsabile della protezione dei dati:

- potrebbe fornire assistenza al titolare del trattamento nella prevenzione e nella gestione dei *data breach*
- potrebbe fornire un parere al titolare del trattamento in merito alla struttura, all'impostazione e alla gestione della documentazione relativa ai *data breach*
- dovrebbe essere informato tempestivamente dell'esistenza di un *data breach*
- dovrebbe essere coinvolto nella gestione dei *data breach* e nel processo di notifica al Garante

# Il ruolo del responsabile del trattamento

**Art. 33, par. 2, del Regolamento**

*«Il responsabile del trattamento informa il titolare del trattamento* ***senza ingiustificato ritardo*** *dopo essere venuto a conoscenza della violazione»*

**Compiti del responsabile del trattamento**

- Non deve valutare la probabilità di rischio derivante dalla violazione
- Deve soltanto stabilire se si è verificata una violazione e quindi informare il titolare del trattamento

Il contratto tra il titolare del trattamento e il responsabile del trattamento dovrebbe indicare le modalità con cui viene assicurato il rispetto delle disposizioni di cui all'art. 33, par. 2, del Regolamento

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Casi pratici di gestione dei *data breach*

**Valutazione del rischio per i diritti e le libertà degli interessati derivante dal *data breach***

**Notifica al Garante e comunicazione agli interessati**

**Misure tecniche e organizzative per porre rimedio al *data breach***

**Misure che avrebbero potuto ridurre il rischio per i diritti e le libertà degli interessati**

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (1)

**Scenario di riferimento**

- Un Ministero ha realizzato un servizio *online* attraverso il quale circa 60.000 dipendenti pubblici possono accedere a corsi di *e-learning*
- Un *hacker*, sfruttando una vulnerabilità di tipo *SQL injection*, riesce ad accedere ai dati contenuti nel *database* degli utenti iscritti al servizio
- Il Ministero non si accorge di aver subìto un attacco informatico in quanto non dispone di strumenti per rilevarlo
- Alcune settimane più tardi, l'*hacker* pubblica in rete una parte dei dati che è riuscito a esfiltrare dal *database* del servizio *online*
- Tra i dati oggetto di pubblicazione ci sono il nome, il cognome, l'indirizzo email e la *password* (sotto forma di *hash*) degli utenti
- Il Ministero non ha previsto una scadenza periodica delle *password*
- Le *password* degli utenti iscritti fino al 30 aprile 2017 (circa 47.000) sono memorizzate sotto forma di *hash* MD5, mentre quelle degli utenti iscritti dopo tale data (circa 13.000) sotto forma di *hash* SSHA256

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (2)

**Elementi considerati per la valutazione del rischio**

| | |
|---|---|
| **Tipo di violazione** | Violazione della riservatezza dei dati causata da un azione intenzionale esterna |
| **Natura, carattere sensibile e volume dei dati personali** | Numero elevato di dati personali, tra cui anche credenziali di autenticazione |
| **Numero di persone fisiche interessate** | Numero elevato di interessati |
| **Facilità di identificazione delle persone fisiche** | I dati personali violati consentono di risalire facilmente all'identità degli interessati |
| **Conseguenze per le persone fisiche** | Perdita di controllo da parte degli interessati sui loro dati personali<br>Furto o usurpazione d'identità |

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (3)

**Valutazione del rischio**

**È PROBABILE CHE CI SIA UN RISCHIO ELEVATO**

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (4)

**Notifica al Garante**

- Il Ministero dovrà notificare il *data breach* al Garante entro 72 ore dal momento in cui ne è venuto "a conoscenza"

**Comunicazione agli interessati**

- Il Ministero dovrà informare gli interessati coinvolti nella violazione inviando due differenti comunicazioni:
  - Interessati con *password* sotto forma di *hash* MD5 → Comunicazione del *data breach* con la raccomandazione di non utilizzare più la *password* compromessa né una simile e di provvedere a modificare le *password* di altri servizi *online* se coincidenti o simili a quella oggetto di violazione
  - Interessati con *password* sotto forma di *hash* SSHA256 → Comunicazione del *data breach*

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (5)

**Misure per porre rimedio al *data breach***

- Blocco immediato dell'accesso ai servizi coinvolti
- Comunicazione tempestiva agli interessati, differenziandone il contenuto in funzione del rischio per gli interessati
- Modifica delle *password* oggetto di violazione, tenendo anche conto che le caselle e-mail degli interessati potrebbero essere state violate

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Casi pratici di gestione dei *data breach*

## Caso A – Compromissione di credenziali di autenticazione (6)

**Misure che avrebbero potuto ridurre il rischio**

- Memorizzazione sicura delle *password*
- Utilizzo di *password* complesse
- Adozione di meccanismi di *strong authentication*
- Utilizzo di *username* diverse dell'*e-mail*
- *Hardening* e *patching* dei sistemi
- *Logging* degli accessi e delle operazioni
- Utilizzo di sistemi di *security information and event management*

# Casi pratici di gestione dei *data breach*

## Caso B – Perdita di dati relativi alla salute (1)

**Scenario di riferimento**

- Un'associazione eroga servizi socio-educativi e socio-assistenziali a bambini con grave disagio familiare
- Il personale dell'associazione utilizza un PC portatile per la redazione e la conservazione dei programmi educativi e riabilitativi dei minori
- Il PC portatile è custodito in una sala adiacente ai locali dell'associazione accessibili al pubblico
- L'accesso al PC portatile è protetto da *password* ma non è stata prevista la cifratura dell'*hard disk* del PC
- In un momento in cui l'accesso ai locali dell'associazione non è presidiato, si verifica il furto del PC portatile
- Al momento del furto, sul PC portatile erano conservati i nominativi, i programmi educativi e rialitativi, le diagnosi e le foto di circa 200 minori in cura negli ultimi 10 anni
- Non sono disponibili *backup* e i dati non possono essere ripristinati

# Casi pratici di gestione dei *data breach*

## Caso B – Perdita di dati relativi alla salute (2)

**Elementi considerati per la valutazione del rischio**

| | |
|---|---|
| **Tipo di violazione** | Violazione della riservatezza e della disponibilità dei dati causata da un azione intenzionale esterna |
| **Natura, carattere sensibile e volume dei dati personali** | Dati relativi alla salute |
| **Facilità di identificazione delle persone fisiche** | I dati personali violati consentono di risalire facilmente all'identità degli interessati |
| **Conseguenze per le persone fisiche** | Perdita del controllo da parte degli interessati sui loro dati personali<br>Discriminazione<br>Pregiudizio alla reputazione |
| **Caratteristiche particolari degli interessati** | Gli interessati coinvolti nella violazione sono minori in condizioni di disagio |

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Casi pratici di gestione dei *data breach*

## Caso B – Perdita di dati relativi alla salute (3)

**Valutazione del rischio**

**È PROBABILE CHE CI SIA UN RISCHIO ELEVATO**

# Casi pratici di gestione dei *data breach*

## Caso B – Perdita di dati relativi alla salute (4)

**Notifica al Garante**

- L’associazione dovrà notificare il *data breach* al Garante entro 72 ore dal momento in cui ne è venuta "a conoscenza"

**Comunicazione agli interessati**

- L’associazione dovrà informare i soggetti che esercitano la responsabilità genitoriale sui minori coinvolti nella violazione

# Casi pratici di gestione dei *data breach*

## Caso B – Perdita di dati relativi alla salute (5)

**Misure che avrebbero potuto ridurre il rischio**

- Custodia del PC portatile in un locale chiuso a chiave
- Cifratura del disco del PC portatile
- Limitazione della conservazione dei dati
- *Backup* periodico dei dati

# Dieci regole per la gestione dei *data breach* (1)

## 5 COSE DA FARE

- Quando si individuano le misure per la sicurezza di un trattamento, considerare i rischi che potrebbero derivare da un eventuale *data breach*
- Effettuare periodicamente *vulnerability assessment* e *patching* dei sistemi
- Trasformare gli utenti da anello debole della catena a prima linea di difesa, incoraggiandoli a segnalare situazioni anomale
- Documentare tutti i ragionamenti che sono alla base delle decisioni prese in risposta a un *data breach*
- Imparare dagli errori propri e degli altri

# Dieci regole per la della gestione dei *data breach* (2)

## 5 COSE DA NON FARE

- Non aspettare che si verifichi un *data breach* per predisporre procedure efficaci per gestirlo
- Non notificare al Garante tutti i *data breach*, ma solo quelli che presentano rischi per i diritti e le libertà degli interessati
- Quando si verifica un *data breach* non pensare agli impatti per il *business*, ma piuttosto ai possibili effetti negativi per gli interessati
- Non sottovalutare i rischi derivanti da un *data breach*
- Non vedere la comunicazione di un *data breach* agli interessati come un'ammissione di colpa, ma piuttosto come uno strumento di trasparenza nei loro confronti