Impact Assessment – DPIA

Uno strumento per la sicurezza informatica e dei dati

Monica Palmirani
CIRSFID, Università di Bologna

Di cosa parliamo oggi

- DPIA: Valutazione d'impatto sulla protezione dei dati
- Template DPIA
- Casi concreti

Considerazione generale

Il dipartimento ICT è uno dei più esposti alle violazioni del GDPR:

Banche dati con dati sensibili	Open data con possibili dati sensibili o personali	Accessi non autorizzati ai dati: problema di credenziali e permessi	Credenziali e Password
Crittografia, anonimizzazione e pseudonimizzazione	Cancellazione corretta dei dati	Backup e rotazione degli archivi	Cloud computing
Intelligenza artificiale o processi di decisione automatica	Profilazione	Sorveglianza	Dati sensibili
Rapporti con i fornitori come responsabili	Sviluppo software e database di testing	Smart working	Dispositivi BYOD

Bussola

- **Base giuridica**
- **Scopo**
- **Pertinenza**
- **Necessità**
- **Limitatezza nel tempo**

- Privacy-by-design → analisi dei dati a priori e integrate nello sviluppo di applicativi
- Privacy-by-default → minimizzazione dei dati necessari per svolgere il compito assegnato
- Accountability → essere sempre in grado di giustificare un trattamento dati nei dettagli e ricondurlo a documentazione certa e legale
- Trasparenza → fornire informazioni per giustificare le scelte fatte

Parametri in gioco con la DPIA

DPIA

- La DPIA non è un documento ma un processo dinamico, circolare, periodico che viene documentato
  - Identificare i rischi
  - Misurarne il pericolo
  - Coordinare le soluzioni senza contraddizioni
  - Gestire le eccezioni in modo consistente
  - Avere un metodo scientifico di analisi critica
  - **Documentare le scelte per poi saper rispondere alla compliance e all'audit**

DEFINIZIONE NORMATIVA

Impact Assessment

- Art. 32, 35, 36, 39

Sezione 3

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 35

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Articolo 35
Valutazione d'impatto sulla protezione dei dati

1.Quando un tipo di trattamento, allorché prevede in particolare l'uso di **nuove tecnologie**, considerati la **natura**, **l'oggetto**, il **contesto** e le **finalità del trattamento**, **può presentare un rischio elevato** per i **diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali**. **Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.**

2.Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il **responsabile della protezione dei dati**, qualora ne sia designato uno.

NOMINARE I RESPONSABILI SUBITO!

Articolo 35
Valutazione d'impatto sulla protezione dei dati

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 **è richiesta in particolare nei casi seguenti**:

a) una valutazione sistematica e globale di aspetti personali relativi a **persone fisiche**, basata su un trattamento **automatizzato**, compresa la **profilazione**, e sulla quale si **fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche**;

→ algoritmi di decisione automatica

b) il **trattamento, su larga scala**, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, **o di dati relativi a condanne penali e a reati di cui all'articolo 10**; o

→ dati sanitari, scolastici, welfare, fiscalità

c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico.**

→ polizia municipale

Articolo 35
Valutazione d'impatto sulla protezione dei dati

5. L'autorità di controllo può inoltre redigere e rendere pubblico un **elenco delle tipologie di trattamenti** per le quali **non è richiesta una valutazione d'impatto sulla protezione dei dati**. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

Articolo 35
Valutazione d'impatto sulla protezione dei dati

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Articolo 35
Valutazione d'impatto sulla protezione dei dati

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei **codici di condotta** approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Articolo 35
Valutazione d'impatto sulla protezione dei dati

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

→**Bisogna prevedere un questionario per gli utenti finali per misurare il rischio di**

- →**frequenza e impatto degli errori nei dati**
- →**frequenza e impatto della perdita dati (data breach)**
- →**frequenza e impatto sui diritti e le libertà individuali dei loro trattamenti**

Art. 32 GDPR

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; (ISO 27001 + business continuity)

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; (disaster recovery)

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. (collaudi)

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. (data breach)

Sanzioni per mancata o errata DPIA

- Chi non rispetta il DPIA perché non lo fa o perché non lo segue 2% del fatturato annuo mondiale per un max 10Meuro

Chi deve fare il DPIA?

- Il titolare con l'aiuto del DPO e dei responsabili
- Definire i ruoli, le mansioni, le azioni da compiere
- Pubblica amministrazione: obbligata a fare la DPIA

Accountability

- Per dimostrare la compliance con la GDPR – accountability si possono utilizzare:
  - Codici di condotta
  - Standard ISO
  - Certificazione di aderenza agli standard ISO

  - Anonimizzazione, crittografia, pseudomizzazione→ abbassano il livello di rischio

Occorre pubblicare il DPIA?

- Non è un obbligo di legge ma non è vietato
- Si può pubblicare integralmente o in parte
- Deve essere trasmesso all'Autorità Garante se è obbligatorio il parere preventivo

Consulto preventivo all'Autorità

Articolo 36 Consultazione preventiva

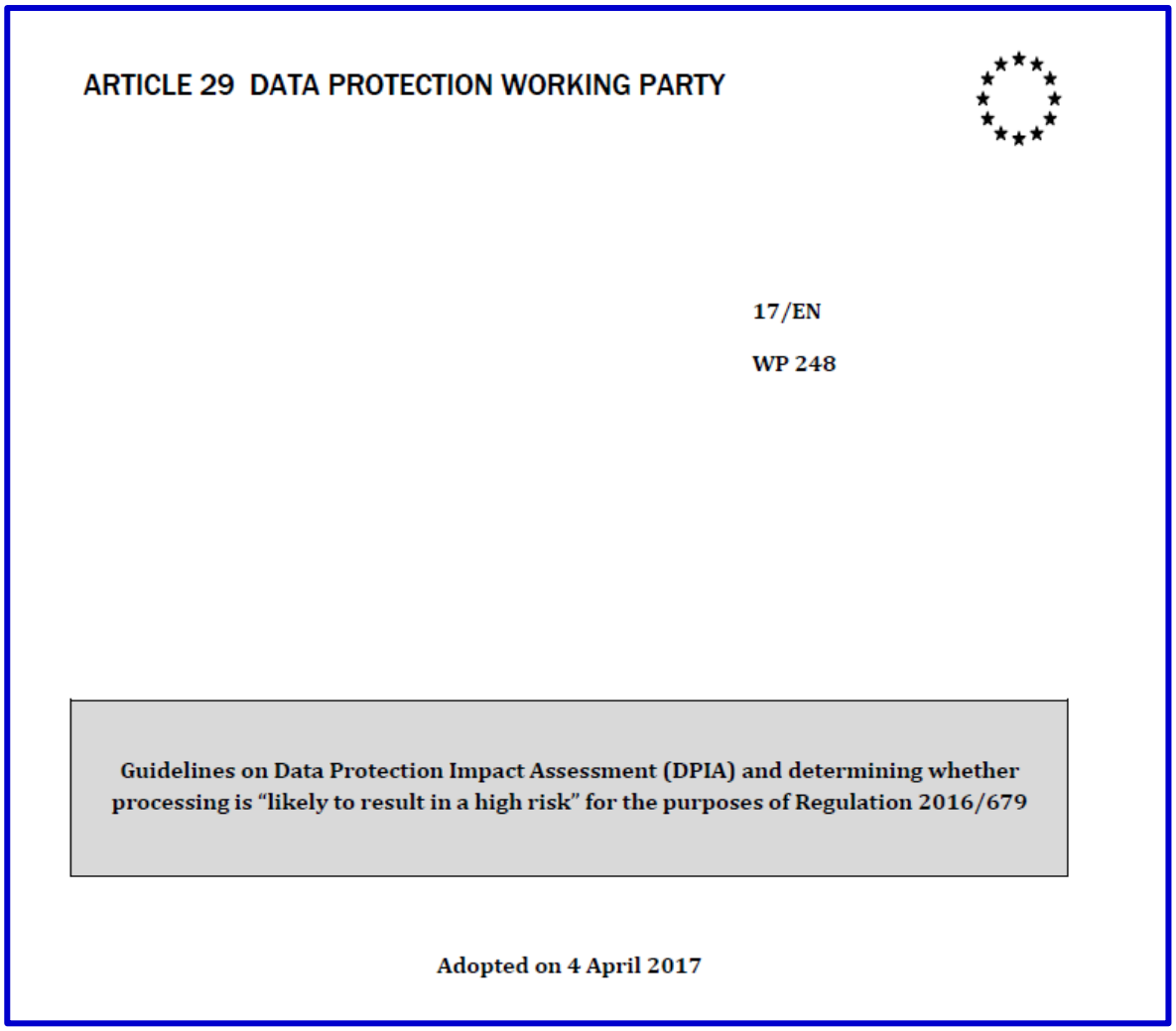
1.Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe **un rischio elevato** in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Ogni quanto occorre fare DPIA?

- Prima del trattamento - preventivamente
- Raccomandato per tutti i processi di trattamento
- L'analisi è obbligatoria per quelli operativi dopo il 25 maggio 2018
- Ogni 3 anni anche se è fortemente consigliato un monitoraggio costante anche con l'aiuto del DPO

LINEE GUIDA

Impact Assessment: Lineeguida



ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248

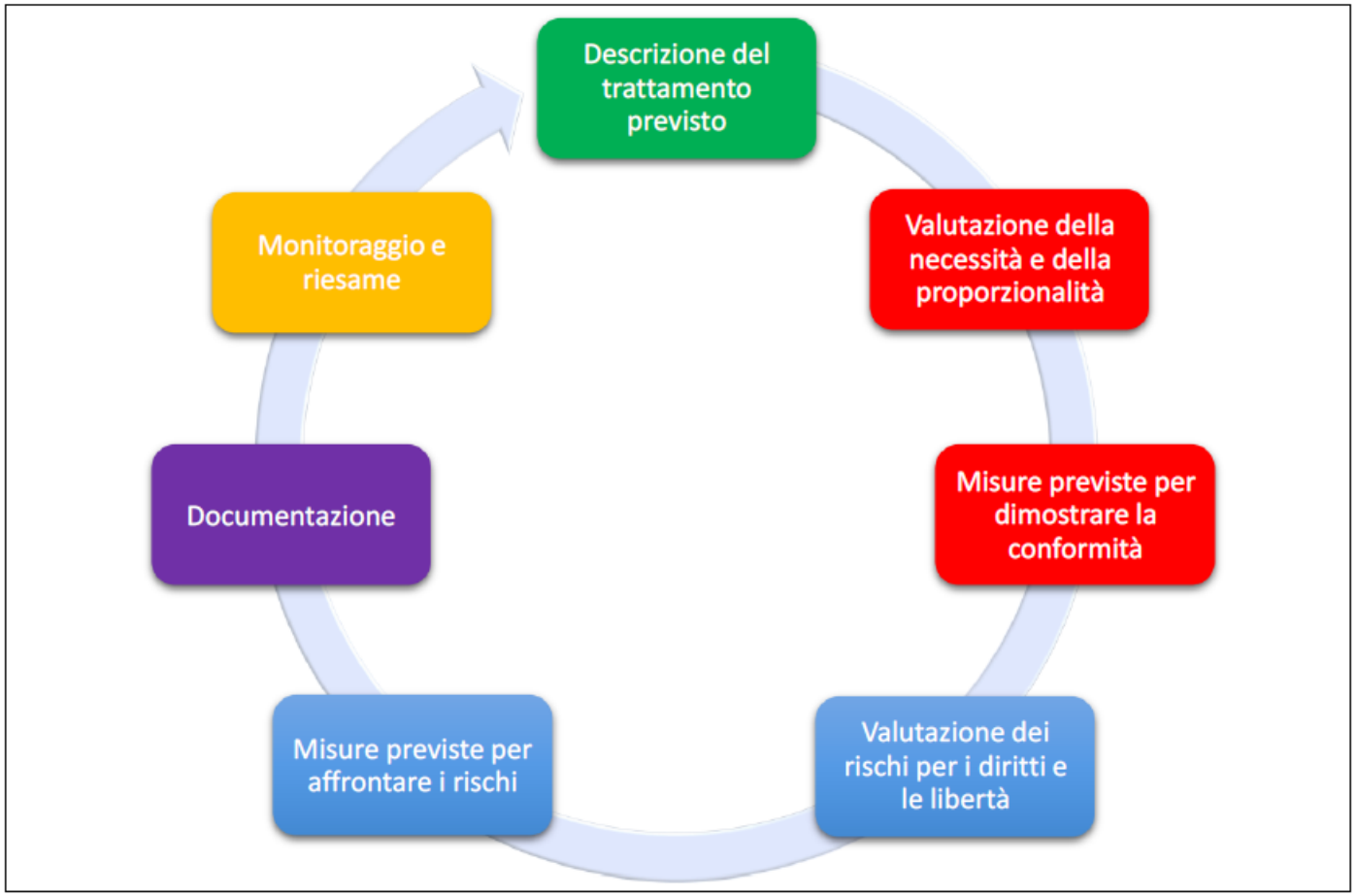
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

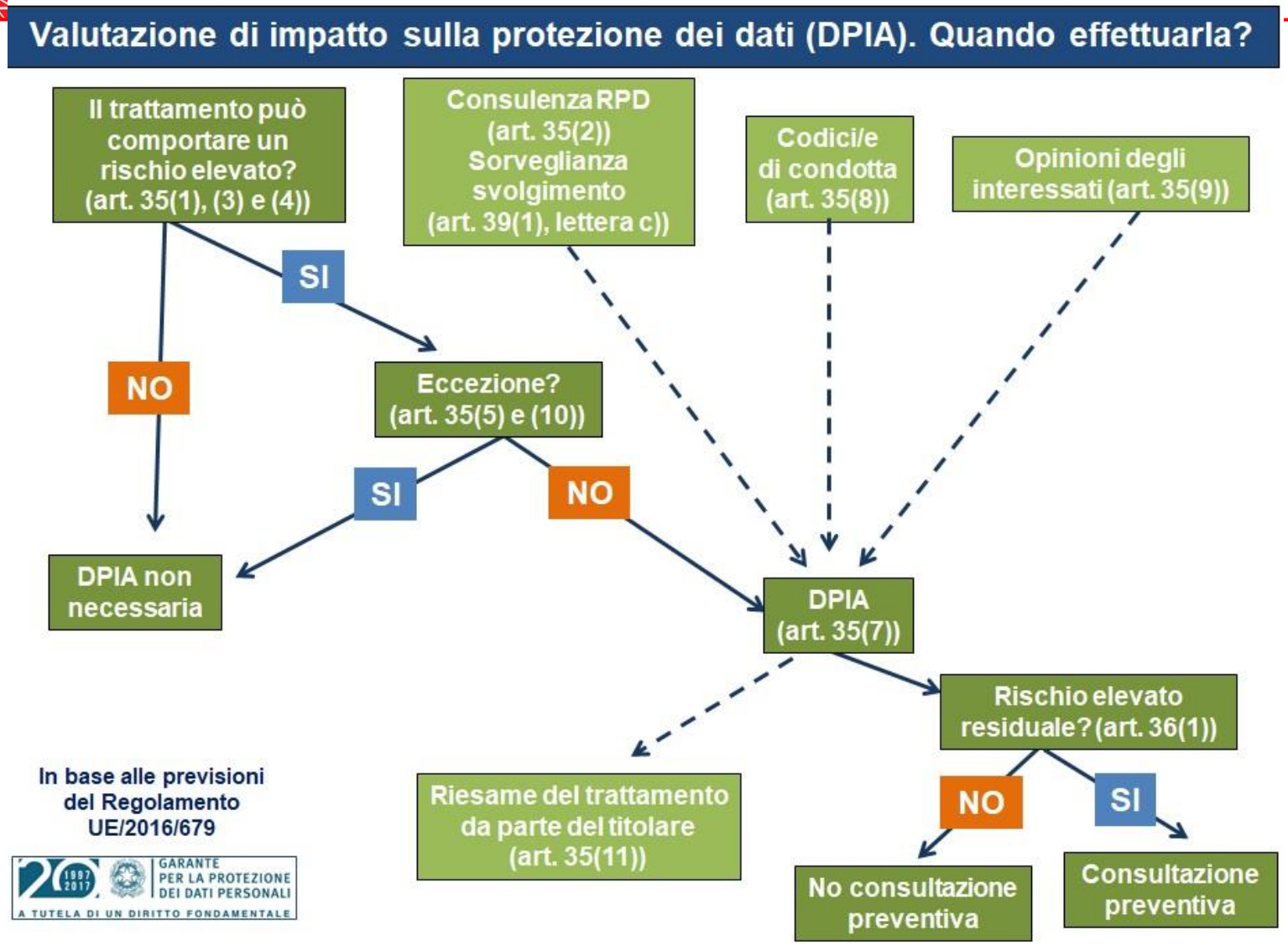
Linee Guida WP29

- Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali4, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24)5. In altre parole, **una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità**.

Metodologia



Diagramma


Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?
Il trattamento può comportare un rischio elevato? (art. 35(1), (3) e (4))
SI
NO
Eccezione? (art. 35(5) e (10))
SI
NO
DPIA non necessaria
Consulenza RPD (art. 35(2)) Sorveglianza svolgimento (art. 39(1), lettera c))
Codici/e di condotta (art. 35(8))
Opinioni degli interessati (art. 35(9))
DPIA (art. 35(7))
Riesame del trattamento da parte del titolare (art. 35(11))
Rischio elevato residuale? (art. 36(1))
NO
SI
No consultazione preventiva
Consultazione preventiva
In base alle previsioni del Regolamento UE/2016/679
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

Cosa deve descrivere il DPIA WP29

- «Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.»
- **Processi che coinvolgono più responsabili necessitano di una descrizione separata**

Per quali trattamenti è obbligatorio

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

Per quali trattamenti è obbligatorio

- Automated-decision making with legal or similar significant effect
- Systematic monitoring – monitoraggio sistematico
- Sensitive data (political opinions) – dati particolari art. 9 GDPR
- Data processed on a large scale: percentuale della popolazione, volume, durata, geolocalizzazione
- Datasets that have been matched or combined
- Data concerning vulnerable data subjects (minori, malati mentali, anziani, impiegati, pazeinti, etc.)
- Innovative use or applying technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract*

Esempi

- valutazione o assegnazione di un punteggio
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
- monitoraggio sistematico
- dati sensibili o dati aventi carattere altamente personale
- trattamento di dati su larga scala
- creazione di corrispondenze o combinazione di insiemi di dati
- dati relativi a interessati vulnerabili
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
- quando il trattamento in sé *«impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto»*

Doppio criterio… ma non sempre

- Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi **due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati**. In generale, il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.
- Tuttavia, in alcuni casi, **un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.**

Valutazione lasciata al titolare

- Per contro, un trattamento può corrispondere ai casi di cui sopra ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati.

Casi

Esempi di trattamento	Possibili criteri pertinenti	È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili. - Trattamento di dati su larga scala.	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	- Monitoraggio sistematico. - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	
La raccolta di dati pubblici dei media sociali per la generazione di profili.	- Valutazione o assegnazione di un punteggio. - Trattamento di dati su larga scala. - Creazione di corrispondenze o combinazione di insiemi di dati. - Dati sensibili o dati aventi carattere estremamente personale.	

Non è il caso di fare DPIA

- **quando il trattamento non è tale da "*presentare un rischio elevato per i diritti e le libertà delle persone fisiche*"**
- **quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati.**
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate
- **qualora un trattamento**, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi **una base giuridica** nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o **sia già stata effettuata una valutazione d'impatto sulla protezione dei dati** nel contesto dell'adozione di tale base giuridica a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- **qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento** per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati

Larga scala

Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili.	No
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	- Trattamento di dati su larga scala.	
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	- Valutazione o assegnazione di un punteggio.	

Percentuale della popolazione

TPER

- Azienda in house 100% S.p.A. partecipata pubblica.
- Traccia i cittadini mediante gli abbonamenti geolocalizzandoli.

- Sì/No?

Convegno universitario

- Convegno internazionale di massimo 1000 persone, raccolta di dati tramite wordpress, presso server di UNIBO, con raccolta anche di dati sensibili (conferenza medica con coinvolgimento di associazioni di malati).
- Sì/No?

Contenuto minimo DPIA

Il contenuto minimo è specificato dall'articolo 35, paragrafo 7, come segue:

- *"a) una **descrizione sistematica** dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
- *b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;*
- *c) una **valutazione dei rischi per i diritti e le libertà degli interessati** di cui al paragrafo 1; e*
- *d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione";*

Definizione di rischio

- «Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.
- La "gestione dei rischi", invece, può essere definita come l’insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.»

Standard ISO

- EN ISO 12100
- ISO/IEC 27000
- UNI ISO 31000:2018 → gestione del rischio

ELEMENTI DA CONSIDERARE NELLA INDIVIDUAZIONE DEL RISCHIO

Risk assessment

- Identificazione ed analisi rischio (Passi 1 e 2)
- Ponderazione rischio (Passo 3)
- Mitigazione rischio (Passi 4 e 5)
- Verifica rischio residuo (Passi 6 e 7)

- Errore→causa→effetto→mitigazione→Verifica

Definizione di rischio

- Per **Pericolo** si intende la proprietà o la qualità di un determinato fattore avente la potenzialità di causare un danno
- Il **Rischio** di un evento accidentale è la combinazione tra la Probabilità (o frequenza) del verificarsi di un dato evento dannoso e la Gravità (detta magnitudo) delle sue conseguenze:
  - frequenza: probabilità che l'evento si verifichi in un determinato intervallo di tempo;
  - magnitudo: entità delle possibili perdite e dei danni conseguenti al verificarsi dell'evento.

Rischio = Frequenza x Magnitudo

- Il Rischio genera un effetto di incertezza sugli obiettivi

[Guida ISO 73:2009, definizione 1.1]

Tipi di rischio

- Eliminabile: e.g., assicurazione
- Riducibile: e.g., mitigazione mediante prevenzione (agisce sulla frequenza) e protezione (agisce sulla magnitude)
- Tollerabile: il rischio è ridotto fino ad un livello accettabile giuridicamente, tecnicamente, funzionalmente

Misurazione

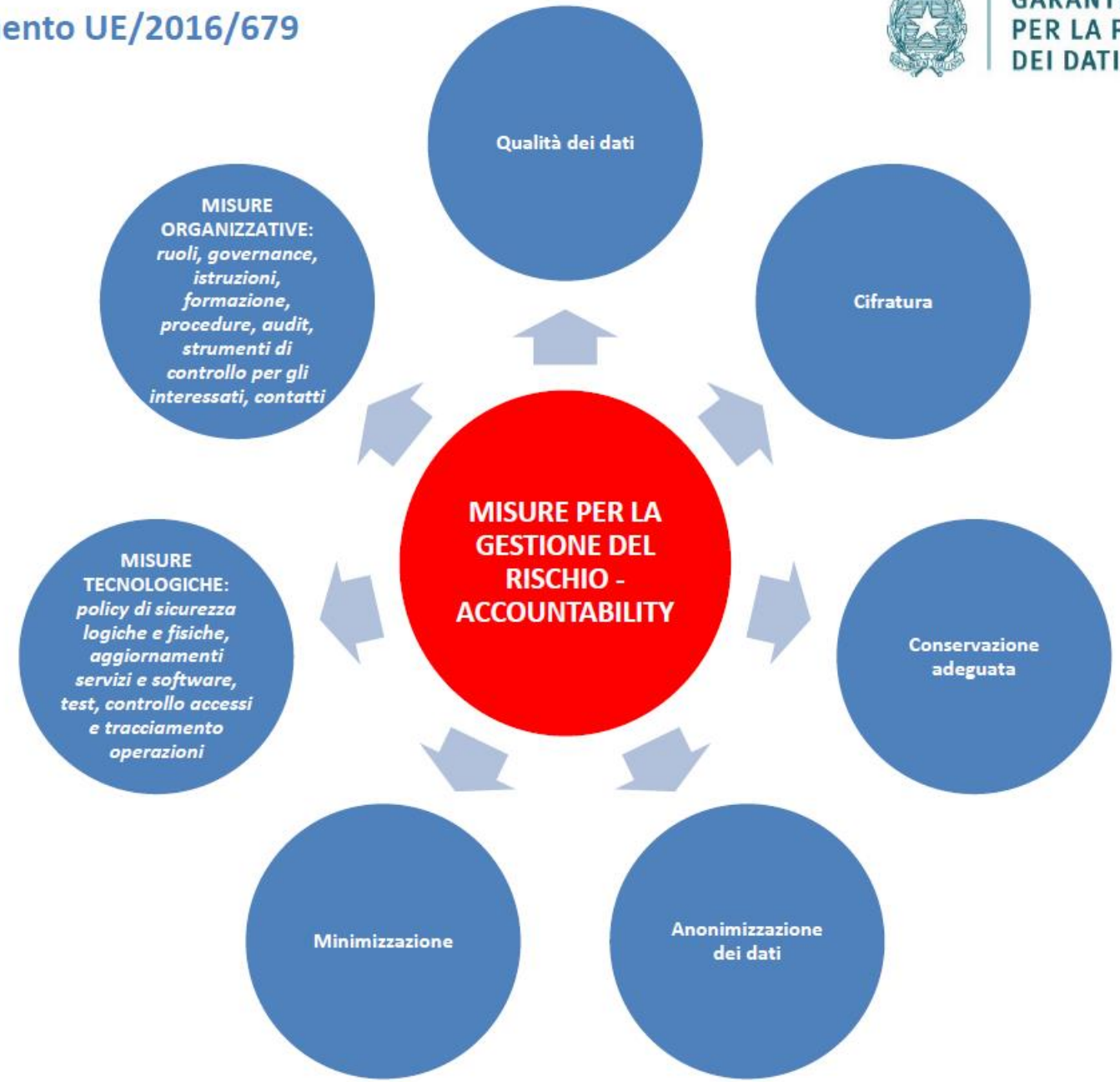
- Magnitudo
  - Estremamente pericoloso
  - Pericoloso
  - Alto
  - Basso
  - Minore
- Temporaneo/permanente
- Probabilità
  - Frequente
  - Occasionale
  - Remota
  - Molto poco probabile

Rischi nel settore dati

Aspetti riguardanti la sicurezza del trattamento

- **DISPONIBILITÀ**
  -distruzione
  -indisponibilità
  -perdita
- **INTEGRITÀ**
  -alterazione
- **RISERVATEZZA**
  -divulgazione
  -accesso


Effetti complessivi del trattamento
Danno per la reputazione
Discriminazione
Furto d'identità
Perdite finanziare
Danni fisici o psicologici
Perdita di controllo dei dati
Altri svantaggi economici o sociali
Impossibilità di esercitare diritti, servizi o opportunità


MISURE PER LA GESTIONE DEL RISCHIO - ACCOUNTABILITY
Qualità dei dati
Cifratura
Conservazione adeguata
Anonimizzazione dei dati
Minimizzazione
MISURE TECNOLOGICHE: policy di sicurezza logiche e fisiche, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni
MISURE ORGANIZZATIVE: ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti

Software o hardware - IoT

- **Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico**, ad esempio un **dispositivo hardware o un software**, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento.

Caso

- Dati della sorveglianza che si sovrascrivono ogni 7 giorni.
- Per evitare data breach meglio crittografarli
- Per garantire la cancellazione meglio avere un software specifico di cancellazione randomica e di rumore casuale. Dipende dal volume dei dati e se attivati da sensori.

- Check lists

Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and portability (Articles 15 and 20);
      - ☐ right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21);
      - ☐ recipients;
      - ☐ processor(s) (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought (Article 35(9)).

DIVERSE METODOLOGIE

Diverse metodologie

- Linee guida EDPS, Spagna, UK: finalità
- Germania: dati
  - Inventario dei dati e su quello si analizzano i rischi
- WP art. 29, Francia: processo
  - Come i dati sono organizzati nel loro ciclo di vita e di processo all'interno di un servizio/prodotto

Finalità

FASES PRINCIPALES DE UNA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

1. Análisis de necesidad

Valoración de la conveniencia de llevar a cabo o no una Evaluación de Impacto en la Protección de Datos Personales.

2. Descripción del proyecto y de los flujos de información

Análisis en profundidad del proyecto obteniendo el detalle de las categorías de datos que se tratan, los usuarios de los mismos, los flujos de información y las tecnologías utilizadas.

3. Identificación de los riesgos

Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan y del daño que causarían si se materializaran.

4. Gestión de los riesgos identificados

Determinación de los controles y las medidas que han de adoptarse para eliminar, mitigar, transferir o aceptar los riesgos detectados.

5. Análisis de cumplimiento normativo

Verificación de que el producto o servicio que se está desarrollando cumple con los requerimientos legales, generales o sectoriales, en materia de protección de datos.

6. Informe final

Relación detallada de los riesgos identificados y de las recomendaciones y propuestas para eliminarlos o mitigarlos. Su destinatario principal es la dirección de la organización.

7. Implantación de las recomendaciones

Decisión sobre las recomendaciones del informe final y las acciones que deben llevarse a cabo. Asignación de los recursos necesarios para su ejecución y del responsable de implantarlas.

8. Revisión y realimentación

Análisis del resultado final para comprobar la efectividad de la EIPD y verificar si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estos resultados se utilizan para realimentar la evaluación de impacto y actualizarla cuando sea necesario.

Consulta con las partes afectadas

Para una correcta identificación de los riesgos, es imprescindible llevar a cabo, a lo largo de todo el proyecto y en los momentos apropiados, consultas con todas aquellas partes que vayan a resultar afectadas por el mismo, tanto internas como externas a la organización.

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN (DERECHOS ARCO)

- ¿Se adoptan las medidas necesarias para garantizar el carácter personalísimo (verificación de la identidad o, en su caso, de la validez de la representación otorgada a un tercero) del ejercicio de los derechos?
- ¿Se han adoptado medidas para acredita minoría de edad?
- ¿Se ha previsto el ejercicio de los derecho forma de acreditar dicha representación?
- ¿Se ha habilitado un medio sencillo y gratu
- Si el responsable dispone de servicios de at ¿se concede la posibilidad de utilizar esto considera acreditada la identidad de los in el responsable para la prestación de estos
- ¿Se conservan los datos personales de tal f los derechos?
- ¿Se han implantado las medidas y procedin los derechos ARCO en los plazos marcados

MODELO PARA DESCRIPCIÓN DE FLUJOS DE INFORMACIÓN

Código de identificación	Descripción	Origen de la información	Destinatarios de la información	Categorías de datos	Finalidad	Causa legitimadora
1						
2						
3						
...						

MODELO PARA GESTIÓN DE RIESGOS

Código de identificación del riesgo	Descripción del riesgo	Nivel de impacto si el riesgo se materializa	Probabilidad de que se materialice	Medidas propuestas	Impacto tras implantación de medidas propuestas	Probabilidad tras implantación medidas propuestas
1						
2						
3						
...						

Partiamo dai dati

The Standard Data Protection Model

A concept for inspection and consultation on the basis of unified protection goals

V.1.0 – Trial version

Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

4 Structure of the Standard Data Protection Model

The Standard Data Protection Model:

- Transfers legal data protection requirements into a catalogue of protection goals,
- Structures the procedures under consideration into the components data, IT-systems and processes,
- Incorporates the classification of data in three tiers of protection levels,
- Complements these with considerations on the level of procedures and IT-systems and
- Provides a systematically derived catalogue of standardised data protection measures, which have been systematically derived from these principles (see Annex).

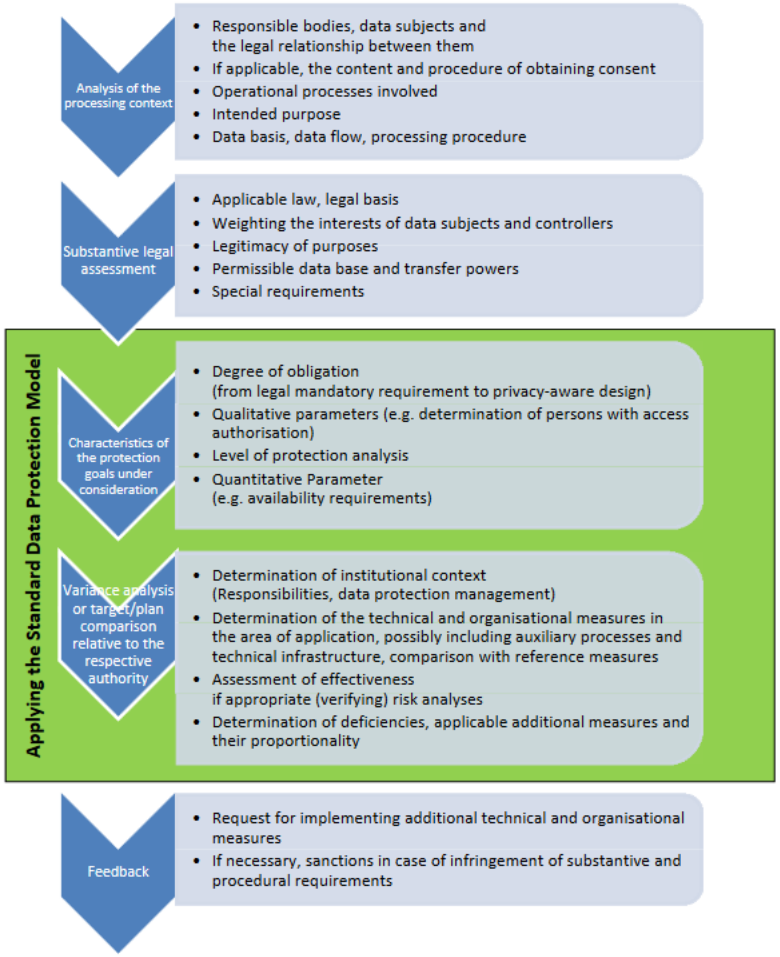
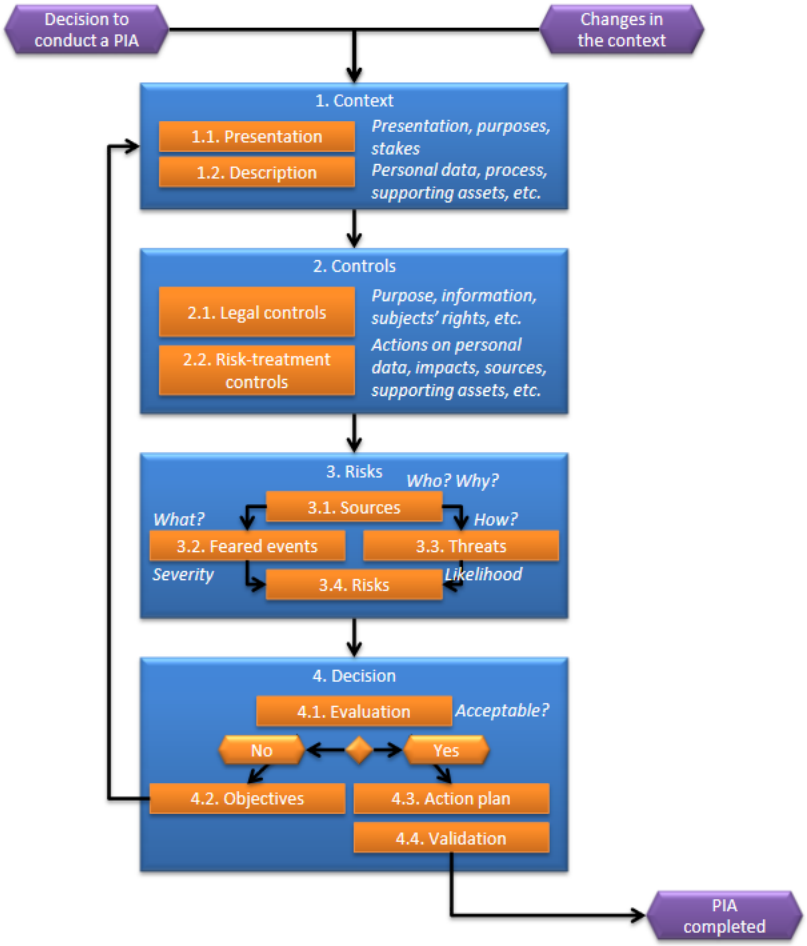


Figure 1. Application of the Standard Data Protection Model within the framework of investigation and consulting activities

1. Availability,
2. Integrity, and
3. Confidentiality.

4. Unlinkability,
5. Transparency, and
6. Intervenability.

Partiamo dai Processi



PIA report

Introduction

- Presentation of the processing of personal data under consideration

Body of the PIA

- Description of the scope
- List of legal controls
- List of risk-treatment controls
- Risk map

Conclusion

- Rationale to validate the PIA

Appendices

- Detailed description of the scope
- Detailed presentation of the controls
- Detailed description of the risks
- Action plan

Overview of the PIA process

1. Identifying the need for a PIA.

The need for a PIA can be identified as part of an organisation's usual project management process or by using the screening questions in annex two of this Code.

2. Describing the information flows.

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information

3. Identifying the privacy and related risks.

Some will be risks to individuals - for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.

Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the DPA, PECR, and the Human Rights Act.

4. Identifying and evaluating privacy solutions.

Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

5. Signing off and recording the PIA outcomes.

Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.

A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

6.Integrating the PIA outcomes back into the project plan.

The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.

Record what you can learn from the PIA for future projects.

Examples of internal stakeholders

- Project management team
  - The team responsible for the overall implementation of a project will play a central role in the PIA process.
- Data protection officer

  If an organisation has a dedicated DPO, they are likely to have a close link to a PIA. Even if project managers are responsible for individual PIAs, the DPO will be able to provide specialist knowledge on privacy issues,
- Engineers, developers and designers
  - The people who will be building a product need to have a clear understanding of how to approach privacy issues. They will also be able to suggest workable privacy solutions to the risks which have been identified.
- Information technology (IT)
  - Will be able to advise on security risks and solutions. The role of IT is not limited to security, and might also include discussions on the usability of any software.
- Procurement
  - If the project will require systems or services to be procured, the needs of the project need to be established before procurement takes place.
- Potential suppliers and data processors
  - If some of the project will be outsourced to a third party, early engagement will help to understand which options are available.
- Communications
  - A PIA can become a useful part of a project's communication strategy. For example, involving communications colleagues in the PIA can help to establish a clear message to the public about a project.

- Customer-facing roles
  - It is important to consult with the people who will have to use a new system or put a policy into practice. They will be able to advise on whether the system will work as intended.
- Corporate governance/compliance
  - Colleagues who work on risk management for an organisation should be able to integrate PIAs into their work. Other areas of compliance can be included in the PIA process.
- Researchers, analysts, and statisticians
  - Information gathered by a new project may be used to analysing customer behaviour or for other statistical purposes. Where relevant, consulting with researchers can lead to more effective safeguards such as Anonymisation.
- Senior management
  - It will be important to involve those with responsibility for signing off or approving a project.

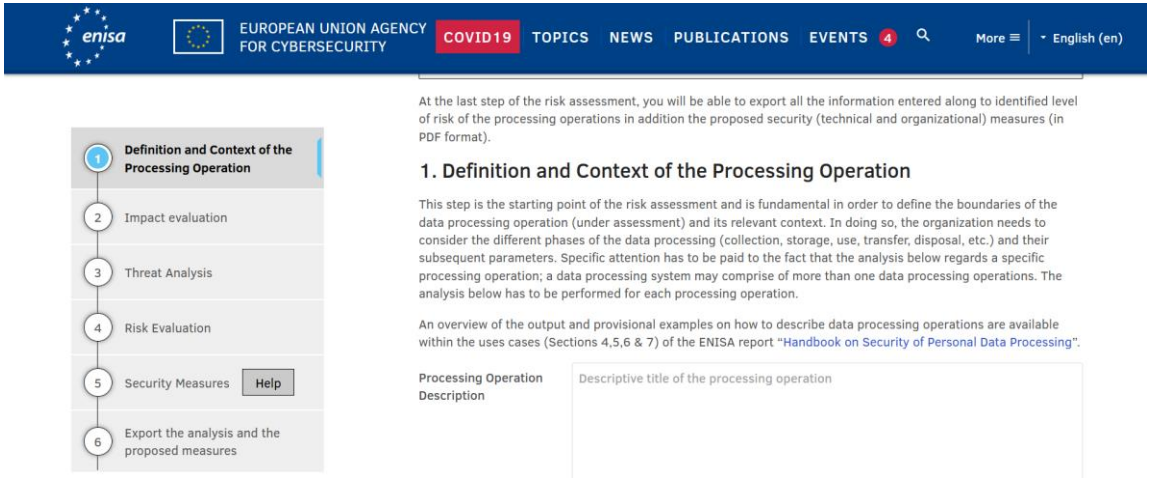
Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

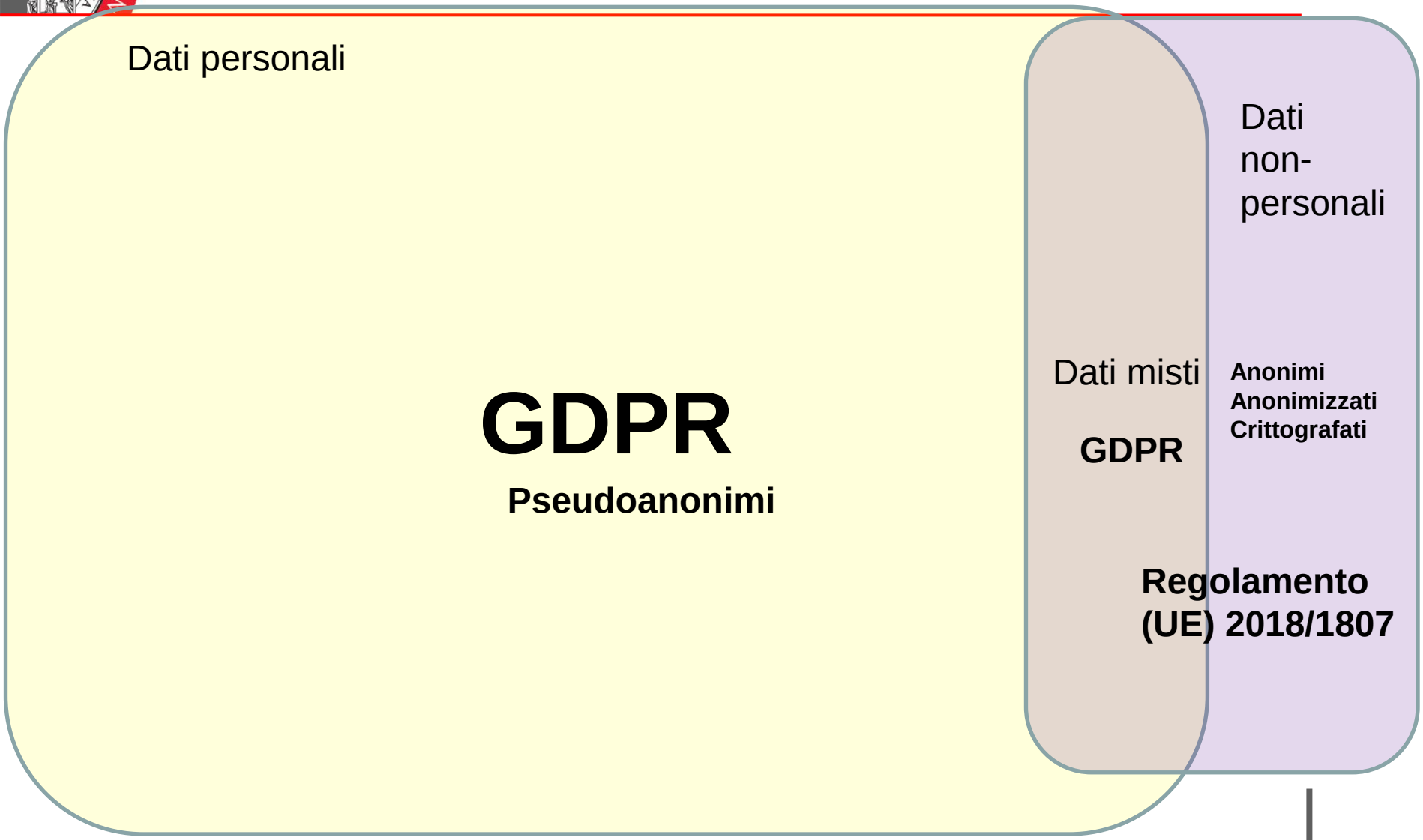
Software

- CNIL – tradotto in Italiano
- UTOPIA
- GoPrivacy
- ENISA
  - https://www.enisa.europa.eu/risk-level-tool/risk



PSEUDONIMIZZAZIONE

Tipi di dati


Dati personali
GDPR
Pseudoanonimi
Dati misti
GDPR
Dati non-personali
Anonimi
Anonimizzati
Crittografati
Regolamento (UE) 2018/1807

Dato personale – Art. 4 GDPR

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Articolo 2, paragrafo 2 Regolamento EU 2018/1807

«Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano **indissolubilmente legati**, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679.»

COMMISSIONE
EUROPEA

Bruxelles, 29.5.2019
COM(2019) 250 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019DC0250&from=EN

Indissolubilmente legato

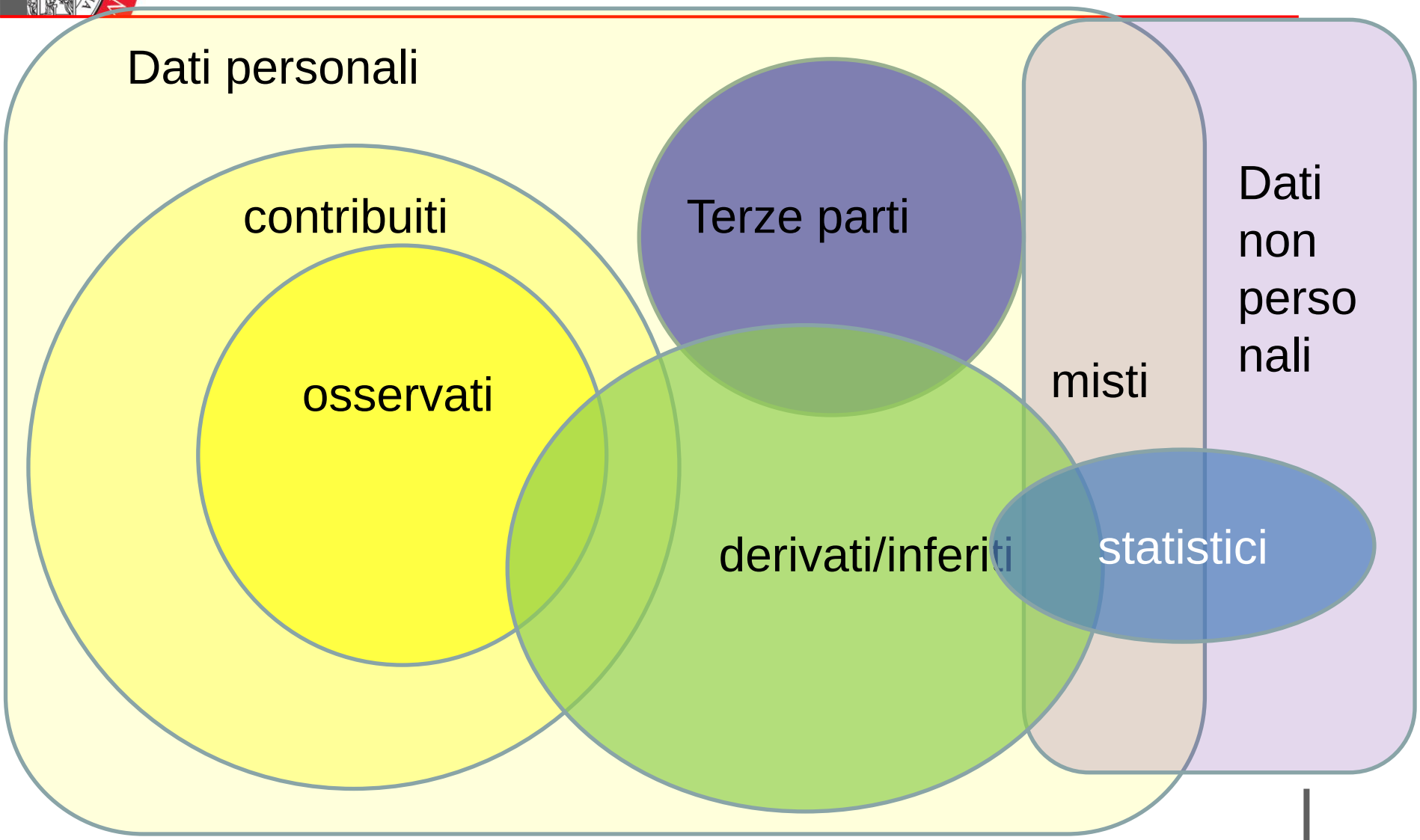
- «Il concetto di "indissolubilmente legato" non è definito da nessuno dei due regolamenti. Ai fini pratici, esso può denotare una situazione in cui un insieme di dati contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile.»

Trattamento dei dati sanitari

I dati sanitari possono rientrare in un insieme di dati misti. Tra gli esempi figurano le cartelle cliniche elettroniche, le sperimentazioni cliniche o gli insieme di dati raccolti dalle varie applicazioni mobili per la salute e il benessere (come le applicazioni per misurare il proprio stato di salute, per ricordarci di prendere le medicine o per rilevare i progressi nella forma fisica)[31]. La divisione esatta tra dati personali e dati non personali in questi insiemi di dati sta diventando sempre più indistinta con gli sviluppi tecnologici. Pertanto, il loro trattamento deve essere conforme al regolamento generale sulla protezione dei dati, in particolare (dal momento che i dati sanitari rappresentano una categoria particolare di dati secondo il regolamento) all'articolo 9 che stabilisce un divieto generale di trattamento di categorie particolari di dati e le eccezioni a questo divieto.

I dati negli insiemi di dati misti contenenti dati sanitari possono essere una preziosa fonte d'informazione, ad es. per ulteriori ricerche mediche, per misurare gli effetti collaterali di un medicinale prescritto, per ottenere statistiche sulle malattie o per sviluppare nuovi servizi o trattamenti sanitari. Tuttavia, occorre ottemperare al regolamento generale sulla protezione dei dati quando si effettua il trattamento iniziale nonché ulteriori trattamenti dei dati. Pertanto, un qualsiasi trattamento simile di dati sanitari deve avere una base giuridica valida[32] e una motivazione adeguata, essere sicuro e fornire garanzie sufficienti.

Tipologia dei dati



Pseudonimizzazione – GDPR – Articolo 4

GDPR: dati personali, dati anonimi, dati pseudoanonimi

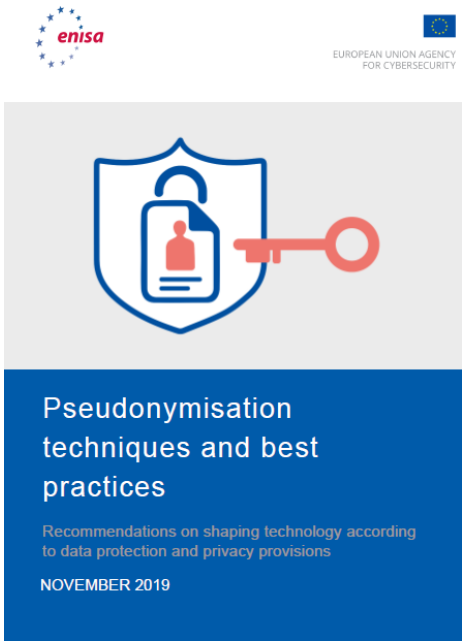
La “pseudonimizzazione”

«5) il 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****»* (art. 4, punto 5 del GDPR)

(28) L'applicazione della pseudonimizzazione ai dati personali può **ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati**. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.

Diversi scenari

- SCENARIO 1: PSEUDONYMISATION FOR INTERNAL USE
- SCENARIO 2: PROCESSOR INVOLVED IN PSEUDONYMISATION
- SCENARIO 3: SENDING PSEUDONYMISED DATA TO A PROCESSOR
- SCENARIO 4: PROCESSOR AS PSEUDONYMISATION ENTITY
- SCENARIO 5: THIRD PARTY AS PSEUDONYMISATION ENTITY
- SCENARIO 6: DATA SUBJECT AS PSEUDONYMISATION ENTITY



Diversi scenari

Figure 1: Pseudonymisation example Scenario 1

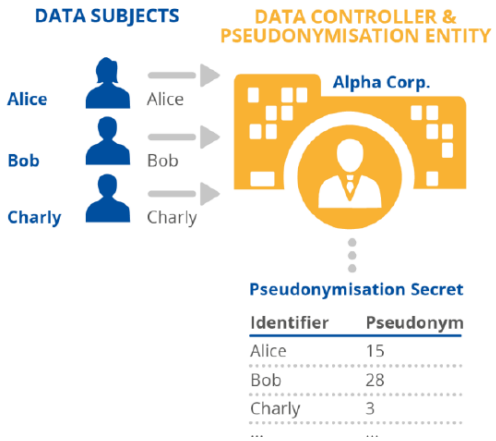


Figure 2: Pseudonymisation example Scenario 2

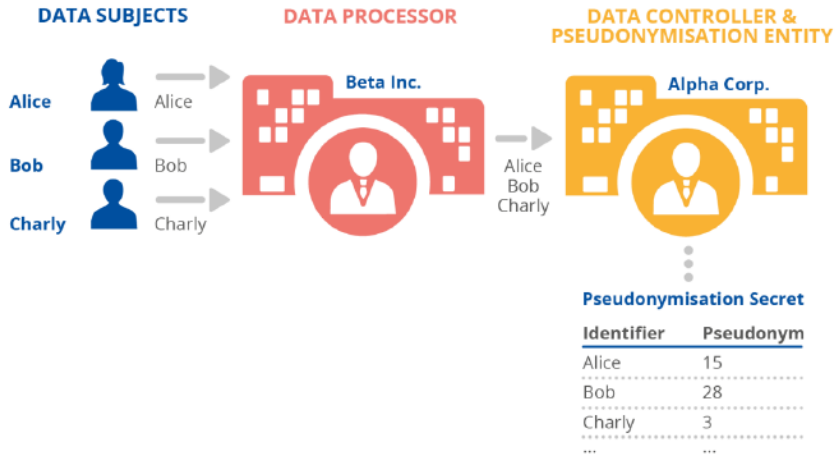
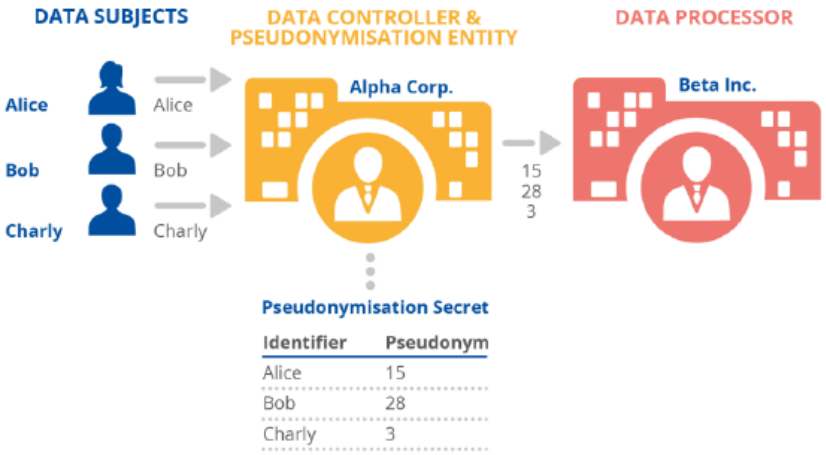
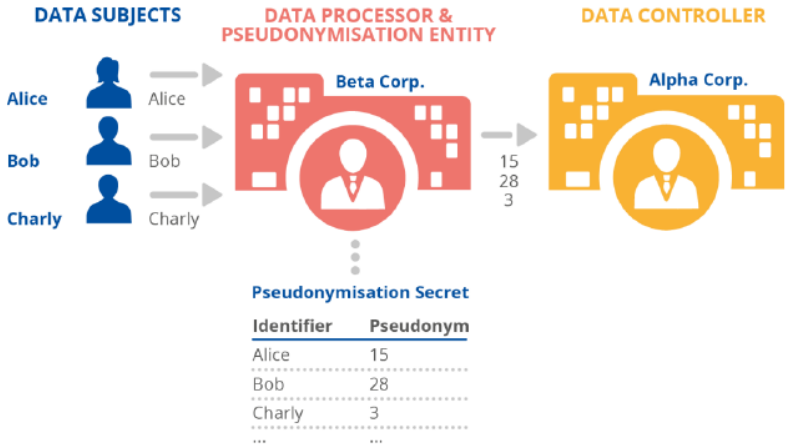


Figure 3: Pseudonymisation example Scenario 3





Le tre operazioni per la pseudonimizzazione

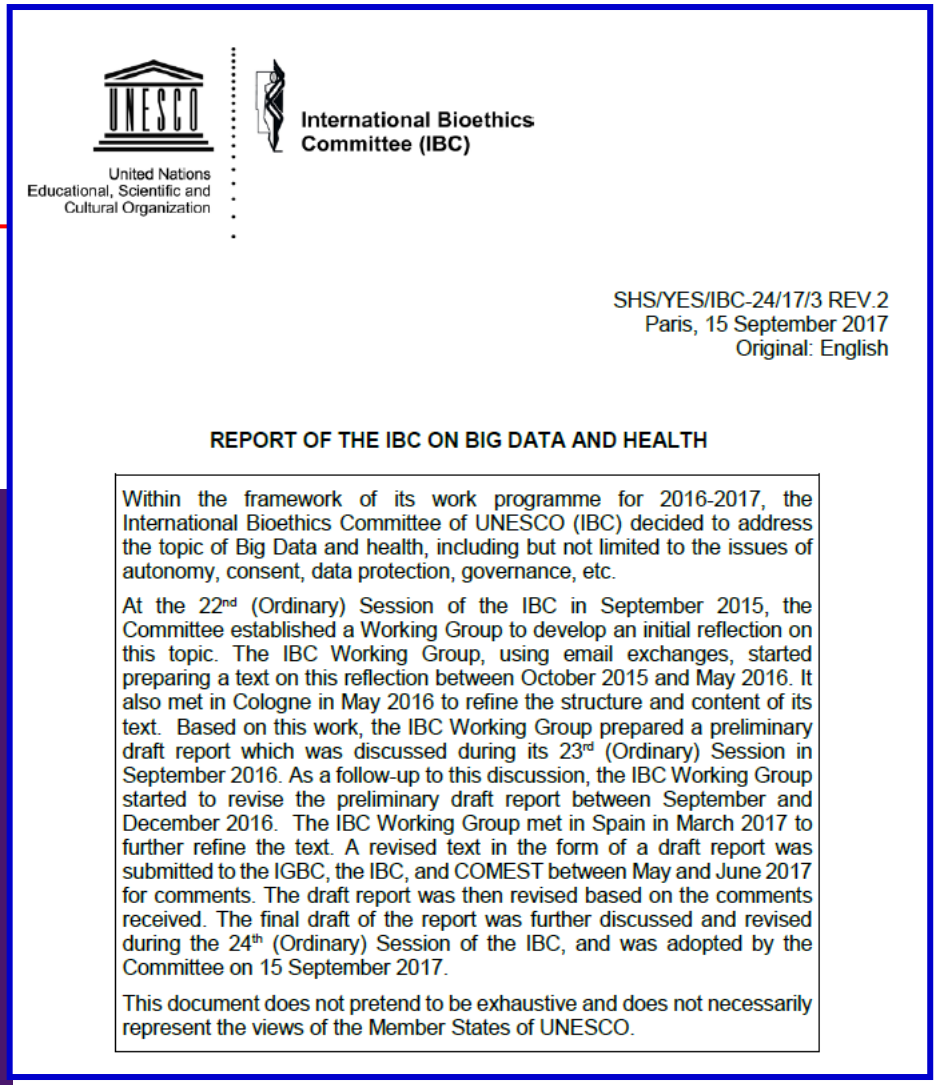
- Divisione: dato personale e altri dati
- Recupero: dei dati identificativi
- Protezione del secreto

- Tutto deve essere in sicurezza e in canale sicuro

Tecniche di Pseudonimizzazione

- Codice/contatore
- Hash (l'hash di un dato personale è ancora un dato personale)
- Mac (è un dato personale)
- Encryption
- Random number generator

ANONIMIZZAZIONE



United Nations
Educational, Scientific and
Cultural Organization

International Bioethics Committee (IBC)

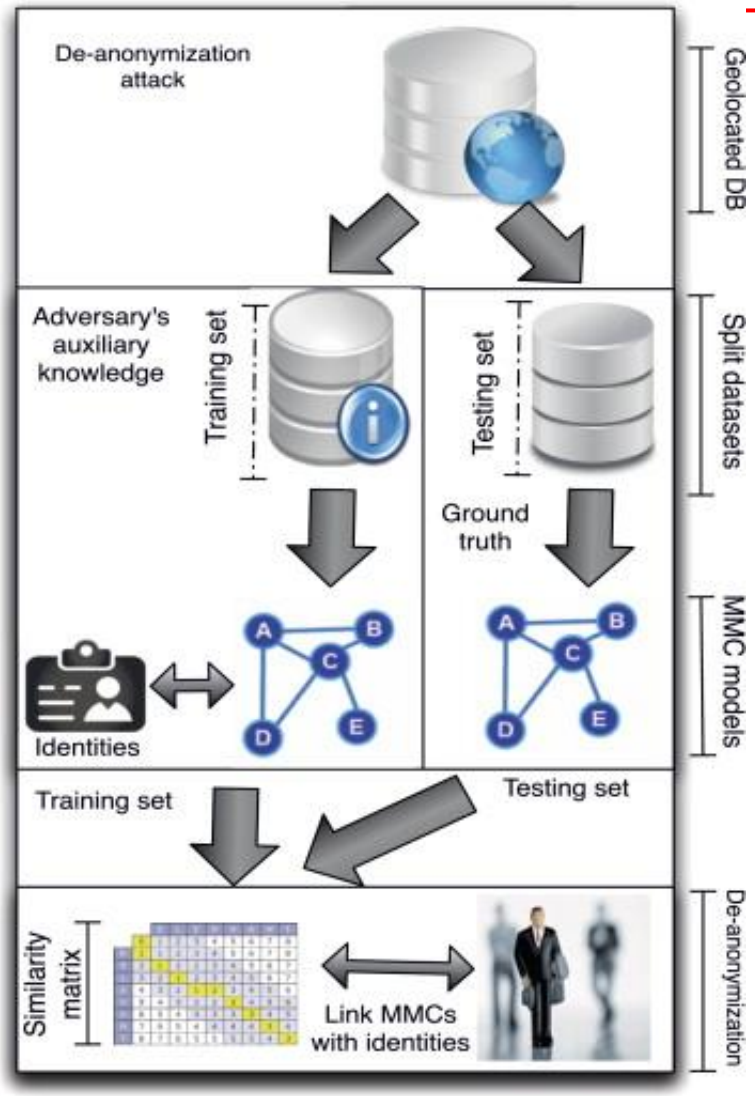
SHS/YES/IBC-24/17/3 REV.2
Paris, 15 September 2017
Original: English

REPORT OF THE IBC ON BIG DATA AND HEALTH

Within the framework of its work programme for 2016-2017, the International Bioethics Committee of UNESCO (IBC) decided to address the topic of Big Data and health, including but not limited to the issues of autonomy, consent, data protection, governance, etc.

At the 22nd (Ordinary) Session of the IBC in September 2015, the Committee established a Working Group to develop an initial reflection on this topic. The IBC Working Group, using email exchanges, started preparing a text on this reflection between October 2015 and May 2016. It also met in Cologne in May 2016 to refine the structure and content of its text. Based on this work, the IBC Working Group prepared a preliminary draft report which was discussed during its 23rd (Ordinary) Session in September 2016. As a follow-up to this discussion, the IBC Working Group started to revise the preliminary draft report between September and December 2016. The IBC Working Group met in Spain in March 2017 to further refine the text. A revised text in the form of a draft report was submitted to the IGBC, the IBC, and COMEST between May and June 2017 for comments. The draft report was then revised based on the comments received. The final draft of the report was further discussed and revised during the 24th (Ordinary) Session of the IBC, and was adopted by the Committee on 15 September 2017.

This document does not pretend to be exhaustive and does not necessarily represent the views of the Member States of UNESCO.


De-anonymization attack
Geolocated DB
Adversary's auxiliary knowledge
Training set
Testing set
Split datasets
Ground truth
A
B
C
D
E
Identities
MMC models
Training set
Testing set
Similarity matrix
Link MMCs with identities
De-anonymization

Rischio De-anonimizzazione

Health Data in an Open World

A report on re-identifying patients in the MBS/PBS dataset and the implications for future releases of Australian government data.

Chris Culnane, Benjamin Rubinstein and Vanessa Teague[1],
School of Computing and Information Systems
The University of Melbourne, 18 Dec 2017
{christopher.culnane, benjamin.rubinstein, vjteague}@unimelb.edu.au

Science. 2013 Jan 18;339(6117):321-4. doi: 10.1126/science.1229566.

Identifying personal genomes by surname inference.

Gymrek M[1], McGuire AL, Golan D, Halperin E, Erlich Y.

Author information

Abstract

Sharing sequencing data sets without identifiers has become a common practice in genomics. Here, we report that surnames can be recovered from personal genomes by profiling short tandem repeats on the Y chromosome (Y-STRs) and querying recreational genetic genealogy databases. We show that a combination of a surname with other types of metadata, such as age and state, can be used to triangulate the identity of the target. A key feature of this technique is that it entirely relies on free, publicly accessible Internet resources. We quantitatively analyze the probability of identification for U.S. males. We further demonstrate the feasibility of this technique by tracing back with high probability the identities of multiple participants in public sequencing projects.

Comment in

Genomic privacy in the information age. [Clin Chem. 2013]
Data re-identification: societal safeguards. [Science. 2013]

PMID: 23329047 DOI: 10.1126/science.1229566

[Indexed for MEDLINE] **Free full text**

- Privacy differenziale, Crittografia omomorfica e il multiparty computation
- Consenso dinamico

These San Diego Scientists Can Predict How You Look Using Only Your Anonymous DNA

Monday, September 4, 2017

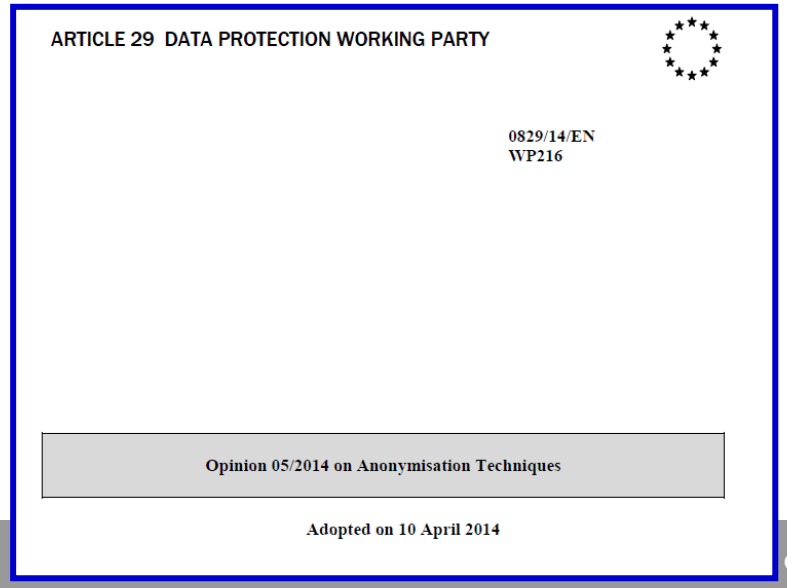
By David Wagner

CREDIT: PNAS

WP216-Anonimizzazione

- The opinion elaborates on the robustness of each technique based on three criteria:
- (i) is it still possible to single out an individual,
- (ii) is it still possible to link records relating to an individual, and
- (iii) can information be inferred concerning an individual?

- ***Singling out***
- ***Linkability***
- ***Inference***


ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

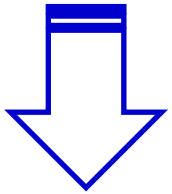
Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

Tecniche di anonimizzazione e pseudonimizzazione

- randomization
  - Noise addition
  - Permutation
  - Differential privacy
- generalization
  - Aggregation and K-anonymity
  - L-diversity/T-closeness
- pseudonymisation (GDPR)
  - Encryption
  - Hash
  - Token
  - Crittografia omomorfica
  - Blind Signature

Art. 29 Working party – Opinion Adopted on 10 April 2014



Permutazione

Anno	Sesso	Professione	Reddito (permutato)
1957	M	Ingegnere	70k
1957	M	Amministratore delegato	5k
1957	M	Disoccupato	43k
1964	M	Ingegnere	100k
1964	M	Dirigente	45k

Tabella 1. Esempio di anonimizzazione inefficace mediante la permutazione di attributi correlati

Aggregazione e k-anonimato

Anno	Sesso	Codice postale	Diagnosi
1957	M	750*	Attacco cardiaco
1957	M	750*	Colesterolo
1957	M	750*	Colesterolo
1964	M	750*	Attacco cardiaco
1964	M	750*	Attacco cardiaco

Tabella 2. Esempio di *k*-anonimizzazione progettata in maniera inadegua

DATI STATISTICI

Articolo 5 GDPR

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a **fini statistici** non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

Articolo 5 GDPR

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a **fini statistici**, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

Art. 89 GDPR

- 1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. **Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo.** Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.
- 2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

Articolo 11 GDPR

"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 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**.

Considerando 162

- (162) Qualora i dati personali siano trattati per **finalità statistiche**, il presente regolamento dovrebbe applicarsi a tale trattamento. Il diritto dell'Unione o degli Stati membri dovrebbe, entro i limiti del presente regolamento, determinare i contenuti statistici, il controllo dell'accesso, le specifiche per il trattamento dei dati personali per finalità statistiche e le misure adeguate per tutelare i diritti e le libertà dell'interessato e per garantire il segreto statistico. Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. Tali risultati statistici possono essere ulteriormente usati per finalità diverse, anche per finalità di ricerca scientifica. La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche.

PORTABILITA’ e ACCESSO

Articolo 15 Diritto di accesso dell'interessato

- Diritto a conoscere i trattamenti in corso, le finalità, dove vengono inviati, se trasferiti all'estero, se alterati o manipolati, il periodo di conservazione, se assoggettati a processo decisionale automatizzato.

Articolo 20 – Portabilità dei dati

«1.L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:»

Abbia dato il consenso o in virtù di un contratto

Articolo 44 Principio generale per il trasferimento

- Trasferimento verso paesi terzi solo in condizioni di garanzia

- Considerando (101) È opportuno che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI RAVENNA

Monica Palmirani
CIRSFID, Università di Bologna
monica.palmirani@unibo.it

www.unibo.it