



UNIVERSITÀ DI PARMA

La protezione dei dati personali nel mondo universitario

Iniziamo con una domanda

Cos'è un 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; (C26, C27, C30)

Alcune curiosità sul GDPR

Quante volte compare la parola privacy nel GDPR?



Questa foto di Autore sconosciuto è concesso in licenza da [CC BY](#)

Alcune curiosità sul GDPR

Qual è l'oggetto del GDPR?

- proteggere i **diritti e le libertà fondamentali delle persone fisiche**, in particolare diritto a protezione dati personali
- favorire la **libera circolazione** dei dati personali nell'Unione Europea

Prima del GDPR: la direttiva 95/46/CE

obiettivo di *“armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri”*

Implementare il *“Right to respect for private and family life”*, European Convention on Human Rights

Recepita con Legge 675/96

Prima del GDPR

Carta dei Diritti
Fondamentali
dell'Unione
Europea
(7/12/2000)

art. 8, “*Protezione dei dati di carattere personale*”, sancisce un diritto autonomo e indipendente rispetto ad altri

D. Lgs. 196/2003 estende diritto riservatezza a protezione dati personali
(Codice Privacy)

Regolamento Generale sulla Protezione dei Dati Personali (Regolamento UE 2016/679)

entra in vigore nel Maggio 2016

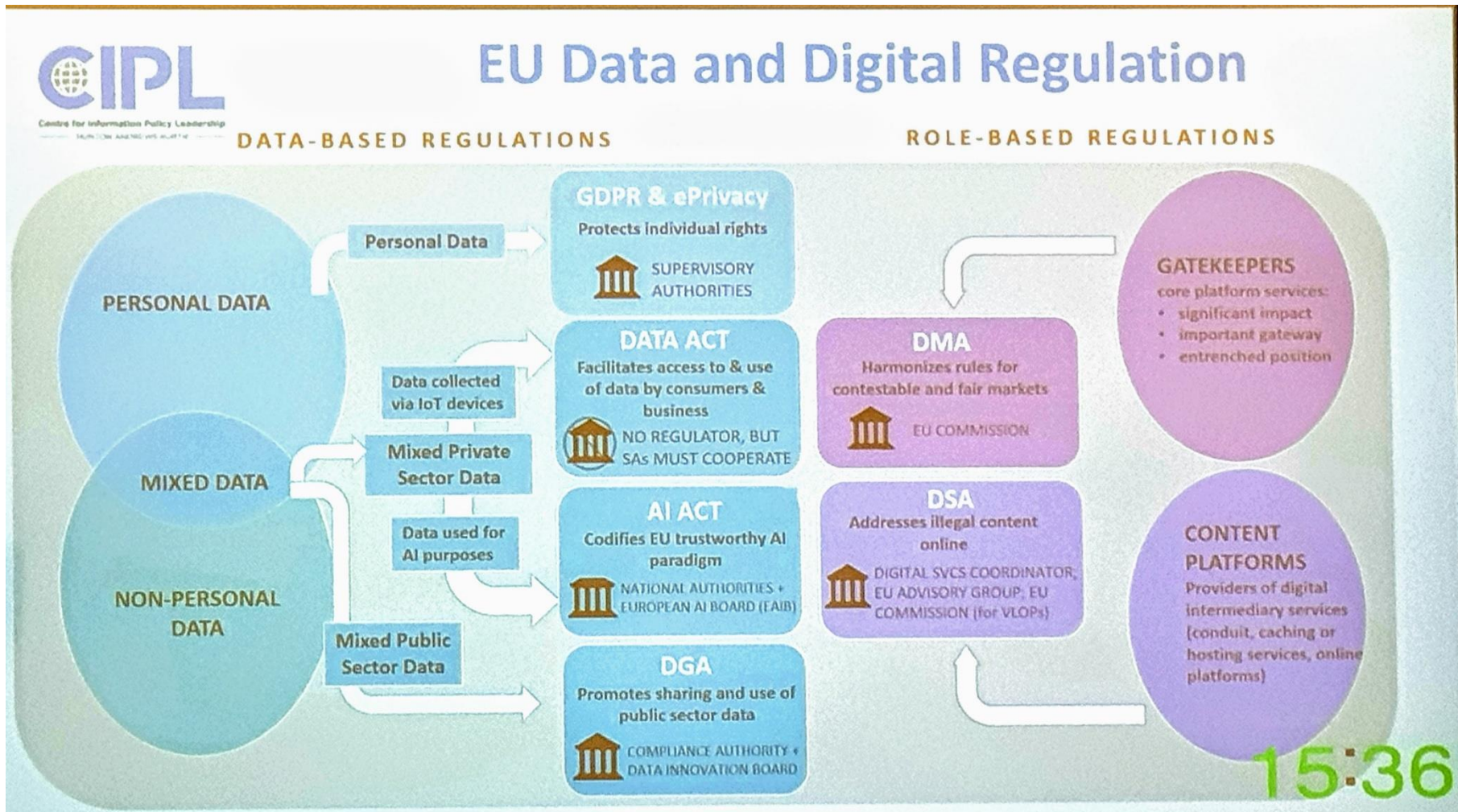
pienamente applicabile nel Maggio 2018

Codice Privacy profondamente modificato con D. Lgs. 101/2018 (e successivi) per essere armonizzato con GDPR

Non solo GDPR



I regolamenti europei sui dati



Le big tech devono sottostare al GDPR?

Ambito di applicazione

trattamento interamente o parzialmente
automatizzato di dati personali

trattamento non automatizzato di dati personali
contenuti in un **archivio** o destinati a figurarvi

titolari localizzati nell'**UE**

titolari localizzati fuori da UE ma **trattamento su
interessati UE**

NO trattamenti ad uso personale

Cosa cambia davvero?

Dal consenso al **controllo** dei propri dati personali

Principio di **accountability** del Titolare

Figura del **DPO**

- il titolare **definisce finalità e mezzi** (essenziali) del trattamento
- il titolare è colui che ha **potere decisionale** sul trattamento e risponde al perché è in corso il trattamento

I principi

Liceità

Correttezza

Trasparenza

Limitazione delle finalità

Limitazione della conservazione

Minimizzazione

Misure di sicurezza



Principio di liceità = basi giuridiche

- ▶ consenso
- ▶ contratto (o condizioni precontrattuali) con l'interessato
- ▶ obbligo legale a cui è soggetto il titolare
- ▶ salvaguardia interessi vitali dell'interessato o di altra persona fisica
- ▶ interesse pubblico - pubblici poteri del titolare
- ▶ legittimo interesse del titolare - se non prevalgono interessi dell'interessato



Categorie particolari di dati personali (ex dati sensibili)

Che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati relativi alla salute

Dati giudiziari

- dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Dati genetici

- Tutti i dati riguardanti le caratteristiche di una persona fisica, ereditarie o acquisite in uno stadio precoce di sviluppo prenatale, quali risultano dall'analisi di un campione biologico dell'individuo, in particolare cromosomica, acido desossiribonucleico (DNA) o acido ribonucleico {RNA} o analisi ed esami o qualsiasi altro elemento che consenta di ottenere informazioni equivalenti.

Dati biometrici

- Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

Tutele e protezione crescenti



Misure di sicurezza adeguate al rischio



Pseudonimizzazione - (art. 4 (5) GDPR)



- 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; (C26, C28-C29)

Dato Anonimo o Pseudonimizzato? (c26 GDPR)

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.



Anonimizzazione - (c26 GDPR)

I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire **informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.**

Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca



Anonimizzazione - (c26 GDPR)

Dati pseudoanonimi = Dati personali

Dati anonimi (impossibili da identificare) ≠ Dati personali

Errore comune:

“Se rimuovo gli identificatori diretti dal set di dati (ad es. nome, indirizzo, numero di previdenza sociale, ecc.), i dati sono anonimizzati ”

Alcuni approfondimenti



DEPLOYING PSEUDONYMISATION TECHNIQUES

The case of the Health Sector

MARCH 2022



DATA PROTECTION ENGINEERING

From Theory to Practice

JANUARY 2022



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENGINEERING PERSONAL DATA PROTECTION IN EU DATA SPACES

JANUARY 2024



Il trattamento dei dati nella ricerca scientifica

Articolo 89

Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (C33, C156-C163)

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.

Il trattamento dei dati nella ricerca scientifica



Il GDPR riconosce il ruolo fondamentale che la ricerca scientifica riveste nel progresso dell'umanità, ma non autorizza il trattamento indiscriminato dei dati.

Ogni trattamento, fin dalla progettazione, deve essere pensato per:


- trattare i dati esclusivamente necessari a quel determinato scopo (minimizzazione);
- proteggere i dati per tutta la durata del trattamento (sicurezza);
- distruggere i dati personali nel momento in cui essi non siano più necessari per le finalità di ricerca scientifica;
- prediligere l'adozione di dati anonimi per sottrarli all'ambito di applicazione del GDPR

Regole essenziali per Il trattamento dei dati nella ricerca scientifica



- **Regola 1:** Se il dato personale non ti serve, cancellalo o distruggilo;
- **Regola 2:** Se ti serve il dato ma non il riferimento alla persona, anonimizzalo;
- **Regola 3:** Se il punto 1 e il punto 2 non sono praticabili, dimostra quello che puoi e non puoi fare per raggiungere gli obiettivi della ricerca.

DPIA



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Scheda aggiornata in base alla
versione delle Linee guida del
WP29 emendata e adottata
il 4 ottobre 2017

**Valutazione di impatto sulla protezione dei dati
(DPIA) – Art. 35 del Regolamento UE/2016/679**

COSA È?
È una procedura prevista dall'articolo 35 del Regolamento UE/2016/679 (RGPD) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?
La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?
La DPIA deve essere condotta prima di procedere al trattamento. Dovrebbe comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari.

CHI?
La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (*Chief Information Security Officer, CISO*) e del responsabile IT.

QUANDO LA DPIA E' OBBLIGATORIA?
In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:

- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

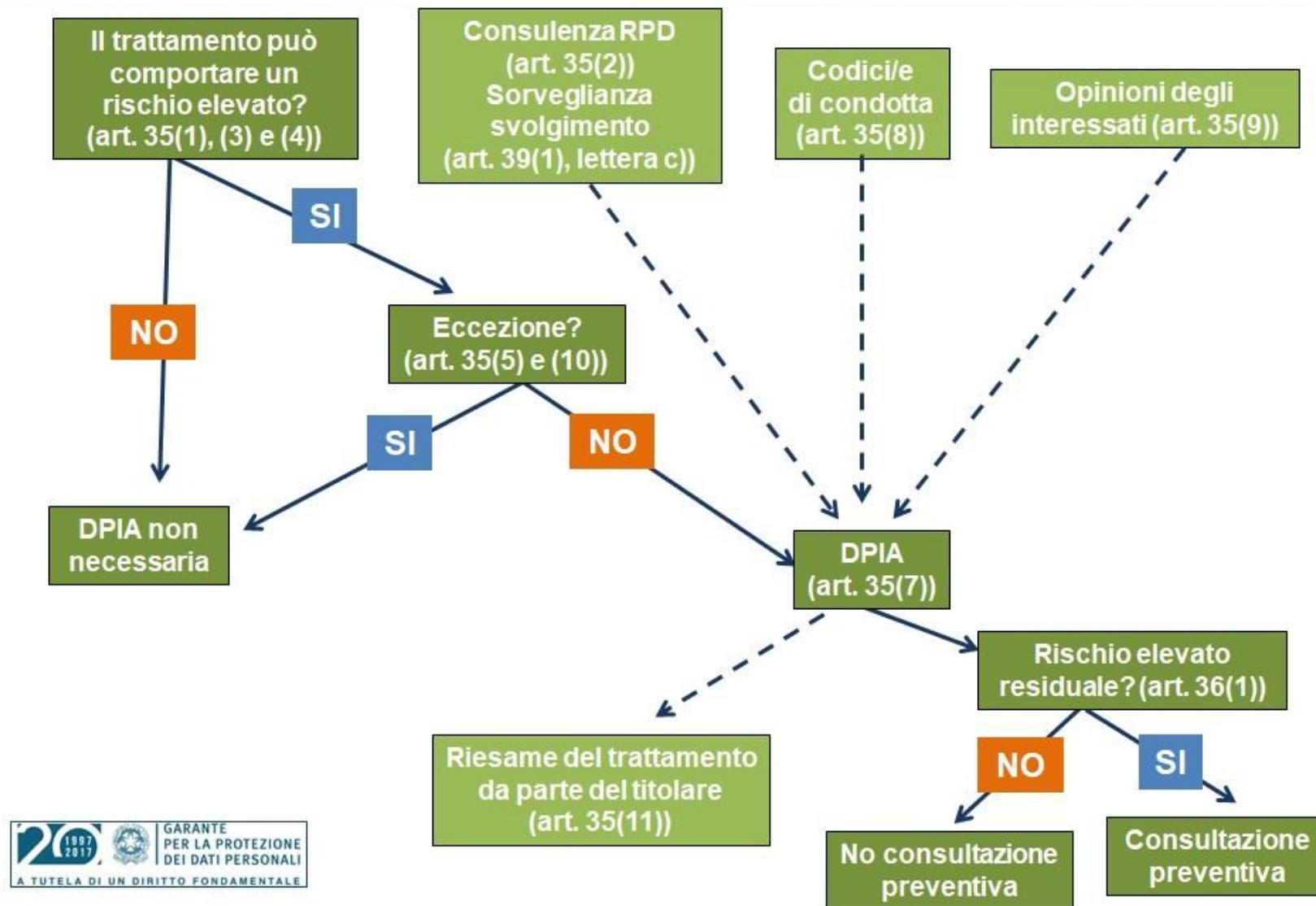
QUANDO LA DPIA NON E' OBBLIGATORIA?
Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON** è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

DPIA

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



Quali sono i limiti della raccolta dati per scopi di sicurezza informatica?

