associazione nazionale dirigenti pubblici
e alte professionalità della scuola

GDPR – 25 MAGGIO 2018

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

www.anp.it

Perché guardate tutti me?

Art. 4
7) **«titolare del trattamento»**:
la persona fisica o giuridica, l'autorità pubblica, [...] che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Perché guardate tutti me?

Art. 4

8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Perché guardate tutti me?

Art. 24 Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi […] 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. [...]

Perchè mi interessa 1 …

Art. 82

- Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il **risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento.
- l titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se **dimostra che l'evento dannoso non gli è in alcun modo imputabile**.

Perchè mi interessa 2 …

Art. 83

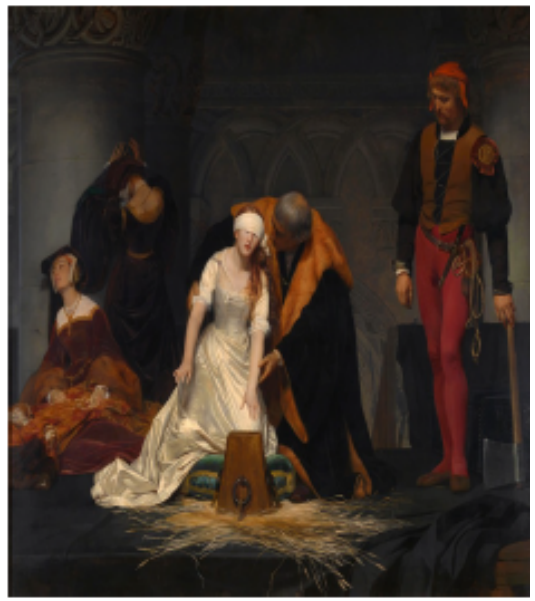
- Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo […] siano in ogni singolo caso **effettive**, **proporzionate** e **dissuasive**

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

Perchè mi interessa 3 …

c. 2 […] il grado di responsabilità [...] tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

- […] l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- c. 4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a **10.000.000** EUR […]
- 5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a **20.000.000** EUR, [...]



Principi 1

Responsabilizzazione
(Accountability)

Non ci sono misure minime:
Più libertà … ma
Responsabilità per le scelte
Valutare i rischi
La medesima logica usata in materia di sicurezza sul lavoro

Principi 2

Il dato è mio!

I dati personali sono … della persona
NON di chi li ha raccolti

Trattare con rispetto:

- No raccolta dati non necessari
- Conservare con cura
- Restituire copia
- Distruggere a scadenza

- **PORTABILITÀ**

Principi 3

Chiedere “per piacere”, salvo quando il trattamento è previsto dalla legge

Art. 4 c. 11) **«consenso dell’interessato»**: qualsiasi **manifestazione di volontà libera**, **specifica**, **informata** e **inequivocabile** dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Principi 4

- Liceità
- Correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Integrità
- Riservatezza
- Limitazione della conservazione

Bisogna poterlo dimostrare

Sopravvivenza 1

Responsabile della protezione dei dati RPD (Data protection Officer) Art. 37

1. Il t**itolare del trattamento** e il responsabile del trattamento **designano sistematicamente** un responsabile della protezione dei dati ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, [...]

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, **un unico responsabile** della protezione dei dati può essere designato **per più autorità pubbliche** o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

7. Il titolare del trattamento o il responsabile del trattamento **pubblica i dati di contatto** del responsabile della protezione dei dati **e li comunica all'autorità di controllo** (Garante privacy per l'Italia)

Art. 39 Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; [...]

b) **sorvegliare l'osservanza del presente regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle **politiche del titolare del trattamento** o del responsabile del trattamento in materia di protezione dei dati personali, compresi **l'attribuzione delle responsabilità**, la **sensibilizzazione e la formazione** del personale che partecipa ai trattamenti e alle connesse attività di controllo

Sopravvivenza

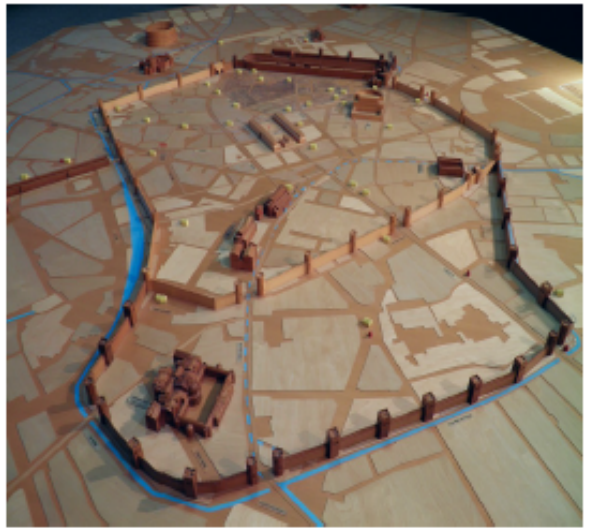
Controllo:

- E’ stato designato un responsabile delle protezione dei dati?
- Sono state assegnate le risorse umane e finanziere per l’attuazione dei compiti del responsabile della protezione dei dati?

Sopravvivenza 2

Art. 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

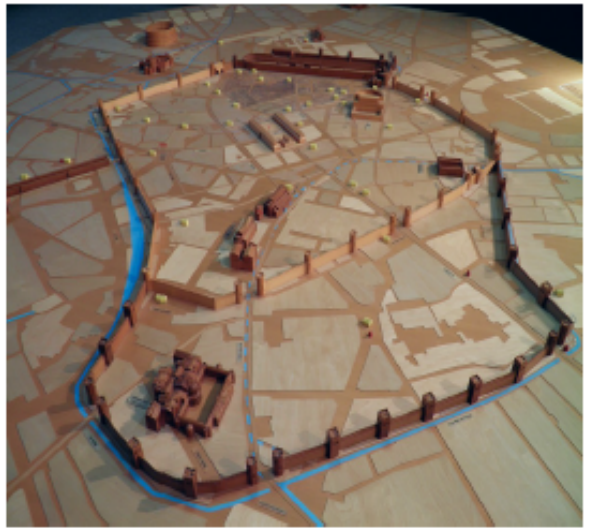
- 1. Tenendo conto dello stato dell'arte e dei costi di attuazione [...] come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, [...] il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad **attuare in modo efficace i principi di protezione dei dati**, [...]



Di Carole Raddato from FRANKFURT, Germany - A model in wood of imperial era Mediolanum, Civico museo archeologico di Milano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=30371091

Mappatura dei trattamenti

2. 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**. [...]

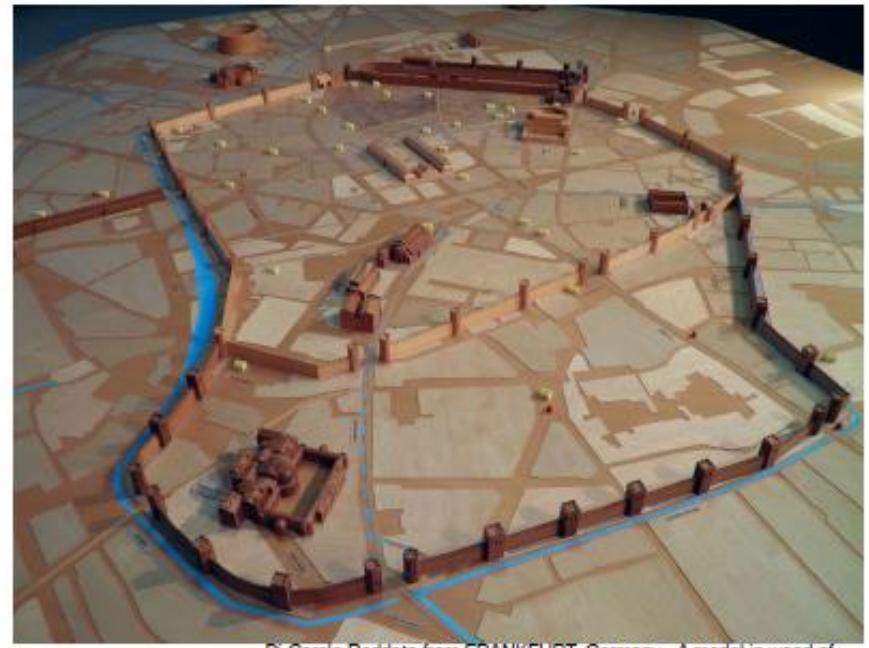


Di Carole Raddato from FRANKFURT, Germany - A model in wood of imperial era Mediolanum, Civico museo archeologico di Milano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=30371091

Mappatura dei trattamenti

Mappatura del trattamento dei dati personali

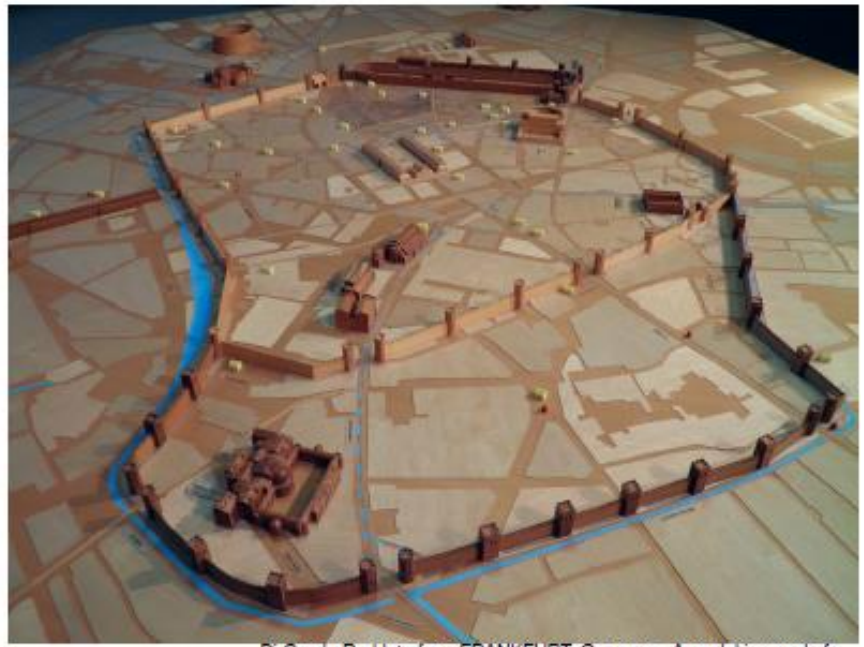
1. Hai individuato i servizi e le entità che elaborano dati personali (interni ed esterni)
2. Hai stabilito l'elenco dei trattamenti **per scopi principali** (non per applicazione o strumento usato!) e tipi di dati trattati



Di Carole Raddato from FRANKFURT, Germany - A model in wood of imperial era Mediolanum, Civico museo archeologico di Milano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=30371091

Mappatura dei trattamenti

3. Per ogni trattamento, quali sono i **soggetti terzi** coinvolti?
4. Sai **dove** vengono memorizzati i dati?
5. Sai **per quanto tempo** vengono conservati i dati? (tenere conto dei tempi di conservazione stabiliti per legge)

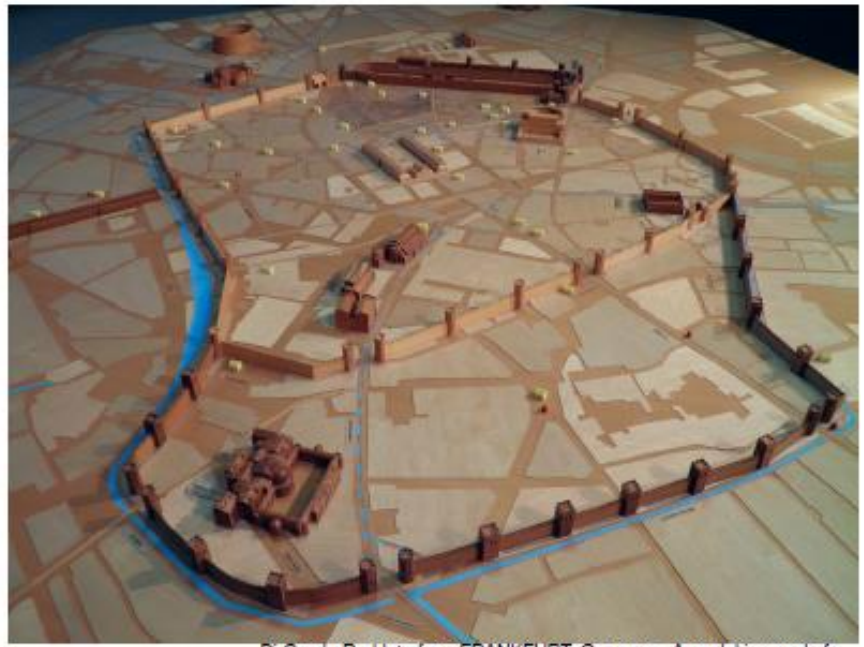


Di Carole Raddato from FRANKFURT, Germany - A model in wood of imperial era Mediolanum, Civico museo archeologico di Milano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=30371091

Mappatura dei trattamenti

6. Hai controllato secondo quali disposizioni normative vengono trattati i dati?

7. Il trattamento dei dati, non imposto dalla legge, è indispensabile? Gli interessati hanno prestato il consenso?



Di Carole Raddato from FRANKFURT, Germany - A model in wood of imperial era Mediolanum, Civico museo archeologico di Milano, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=30371091

Consenso e informativa

Verificare che l'informativa utilizzata per la raccolta del consenso al trattamento dei dati personali sia conforme alle nuove previsioni normative: **le indicazioni degli artt. 13 e 14 sono tassative**

Art. 13 – dati raccolti presso l'interessato

a) l'identità e i dati di contatto del titolare del trattamento [...];
b) i dati di contatto del responsabile della protezione dei dati, [...];
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

Consenso e informativa

e) gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di **trasferire dati personali a un paese terzo** o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione [...]
(ad esempio nel caso di utilizzo di Google education e simili)

Consenso e informativa

Ulteriori informazioni obbligatorie (art. 13 c. 2)
a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la **rettifica o la cancellazione** degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al **diritto alla portabilità** dei dati

Consenso e informativa

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati (esempio: nel caso di viaggi d'istruzione);

Consenso e informativa

Art. 13 c. 3. Qualora il titolare del trattamento intenda **trattare ulteriormente** i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2

Consenso e informativa

Art. 13 c. 4.

I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui **l'interessato dispone già delle informazioni**.

Consenso e informativa

Art. 4 c. 1 numero 11)
«consenso dell'interessato»:

qualsiasi manifestazione di volontà **libera**, **specifica**, **informata** e **inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante **dichiarazione o azione positiva inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento;

Sopravvivenza 4

Primi passi e priorità delle azioni

1. Hai impostato i primi passi per proteggere le persone coinvolte nei vostri trattamenti?

2. Hai identificato i trattamenti a rischio?

Primi passi e priorità delle azioni

Gestione dei rischi

1. Hai messo in atto misure minime per soddisfare i principali rischi e le minacce per la privacy degli interessati ai trattamenti?

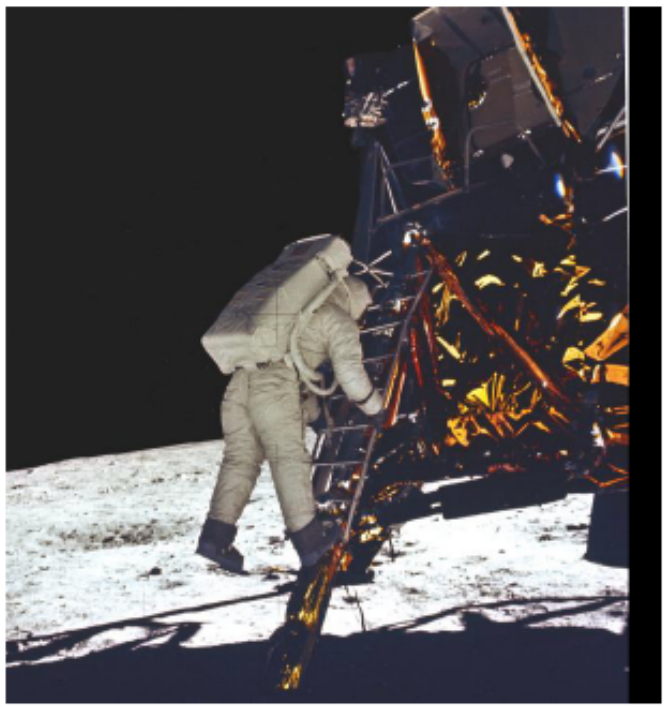
2. Hai identificato fonti di rischio presenti, probabili o future?

Primi passi e priorità delle azioni

Organizzare processi interni

1. Puoi dire di aver ridotto al minimo la raccolta di dati personali?
2. Hai organizzato corsi di formazione per il personale interno alla tua organizzazione, hai predisposto un piano di comunicazione con i tuoi dipendenti?
3. Sei in grado di trattare reclami delle persone interessate per l'esercizio dei loro diritti? (accesso, rettifica, opposizione, diritto alla portabilità, revoca del consenso)

- 4. E' definita un procedura di intervento in caso di incidente sui dati?



associazione nazionale dirigenti pubblici e alte professionalità della scuola

Documento di conformità

La documentazione in tuo possesso ti consente di dimostrare l'adempimento agli obblighi previsti dal regolamento europeo?

Documenti e supporto

Documenti e programmi disponibili:

- Modello di nomina del RPD (DPO)
- Modello di comunicazione al Garante
- Modelli del registro per il trattamento dei dati (in francese)
- Un modello di registro in italiano

segue

Documenti e supporto

Il garante per la privacy francese ha rilasciato un programma per monitorare il processo di conformità, lo strumento è open source ed è già stato tradotto in italiano.
https://www.cnil.fr/fr

si scarica da qui il file appimage per linux
https://www.cnil.fr/fr/les-outils-de-la-conformite

Documenti e supporto

- L'Autorità del Regno unito ha messo a disposizione una serie di informazioni e strumenti (in inglese):

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Grazie per l’attenzione

Buon viaggio … ma

ANP non vi abbandona