Privacy by design

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Membro del Comitato Scientifico del CLUSIT.
Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni.
Oltre 170 corsi e seminari tenuti presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, ABI...; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
Ha all'attivo oltre 800 articoli e collaborazioni con oltre 40 testate.
Ha pubblicato 26 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 28 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT.
Socio e già proboviro di AIEA è socio del CLUSIT, di DFA e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.europrivacy.info .
Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Note sul copyright

Alcuni testi derivano da queste mie pubblicazioni

Privacy by design

Privacy by design

(78) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

Privacy by design

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)

1. 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.*

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. 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.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Principi fondamentali

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security — Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. Visibility and Transparency — Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy — Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Un esempio: soluzioni tecniche

2 Engineering Privacy

- 2.1 Prior art on privacy engineering
- 2.2 Deriving privacy and data protection principles from the legal framework
- 2.3 Definition of the context and objectives
- 2.4 Methodologies
- 2.5 Evaluation means

3 Privacy Design Strategies

- 3.1 Software design patterns, strategies, and technologies
- 3.2 Eight privacy design strategies

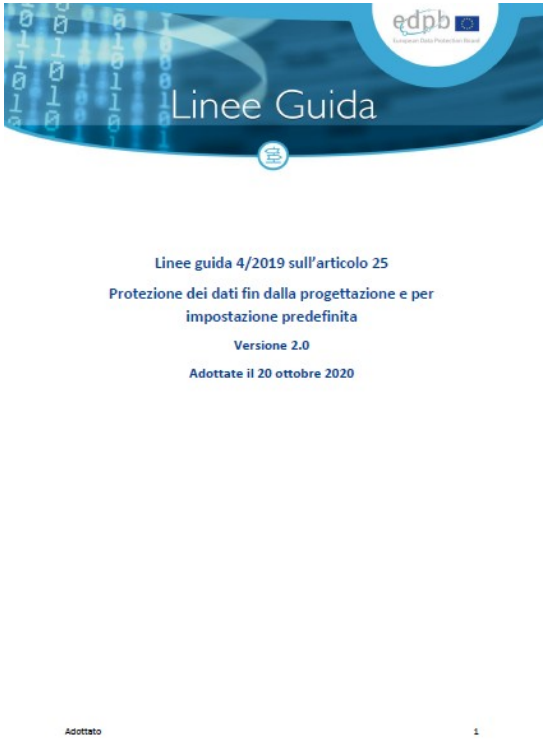
4 Privacy Techniques

- 4.1 Authentication
- 4.2 Attribute based credentials
- 4.3 Secure private communications
- 4.4 Communications anonymity and pseudonymity
- 4.5 Privacy in databases
- 4.6 Technologies for respondent privacy: statistical disclosure control
- 4.7 Technologies for owner privacy: privacy-preserving data mining
- 4.8 Technologies for user privacy: private information
- 4.9 Storage privacy
- 4.10 Privacy-preserving computations
- 4.11 Transparency-enhancing techniques acy: private information

Certificazione (pre GDPR)

Principle 1 – Proactive not reactive; preventative not remedial **(7 criteria; 18 controls)**	The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
Assessment criteria	**Illustrative control activities**
1.1 Privacy Governance - Responsibility and Accountability for Policies and Procedures Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the organization's privacy policies and procedures.	**1.1.1 Accountability for Privacy** The organization assigns responsibility for privacy policies to a designated person who is a senior member of the organization, such as a corporate privacy officer. **1.1.2 Documented Roles and Responsibilities for Privacy** The responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include the following: • Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required; • Formulating and maintaining the organization's privacy policies; • Monitoring and updating the organization's privacy policies; • Delegating authority for enforcing the organization's privacy policies; • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices; and • Reporting to the leadership team on the privacy program, privacy incidents/breaches, any relevant metrics, and compliance, on a periodic basis.

Ambito di applicazione



- La DPbDD (protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita) è un requisito anche per i sistemi di trattamento già esistenti all'entrata in vigore del RGPD;

Ambito di applicazione

- Il fulcro della disposizione è garantire una adeguata ed efficace protezione dei dati fin dalla progettazione e una protezione per impostazione predefinita, il che significa che **i titolari dovrebbero essere in grado di dimostrare** che incorporano nel trattamento le misure e le garanzie adeguate ad assicurare l'efficacia dei **principi di protezione dei dati**, dei diritti e delle libertà **degli interessati**.

2.1.1. Obbligo del titolare del trattamento di attuare ***misure tecniche e organizzative adeguate*** *e le* ***necessarie garanzie*** *nel trattamento*

- misure tecniche e organizzative e necessarie garanzie → *qualsiasi metodo o mezzo che un titolare può impiegare nel trattamento.*
- adeguatezza → *attuare efficacemente i principi di protezione dei dati*
- garanzia e misura tecnica od organizzativa → *tutto ciò che è compreso fra l'uso di soluzioni tecniche avanzate e la formazione di base del personale →….*

Misure tecniche e organizzative adeguate…

→…. Ne sono esempi idonei, a seconda del contesto e dei rischi associati al trattamento in questione:

- la pseudonimizzazione dei dati personali
- la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico
- la possibilità per gli interessati di intervenire nel trattamento
- la fornitura di informazioni sulla conservazione dei dati personali
- la disponibilità di sistemi di rilevamento di malware
- la formazione dei dipendenti sull'«igiene informatica» di base
- l'istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni
- l'obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati, ecc.

2.1.2 Volte ad attuare i principi di protezione dei dati in modo efficace e tutelare i diritti e le libertà degli interessati

- principi di protezione dei dati → articolo 5
- «liceità, correttezza e trasparenza»
- «limitazione della finalità»
- «minimizzazione dei dati»
- «esattezza»
- «limitazione della conservazione»
- «integrità e riservatezza»

Principi di protezione

Articolo 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono: (C39)

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»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

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»);

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»).

I diritti e le libertà degli interessati


7.4.2016 IT Gazzetta ufficiale dell'Unione europea C 202/389

CARTA DEI DIRITTI FONDAMENTALI
DELL'UNIONE EUROPEA

(2016/C 202/02)

*2.1.2 Volte ad attuare i principi di protezione dei dati in modo efficace e tutelare **i diritti e le libertà degli interessati***

- diritti e le libertà fondamentali **delle persone fisiche** → Carta dei diritti fondamentali dell'UE
  - TITOLO I DIGNITÀ
  - TITOLO II LIBERTÀ
  - TITOLO III UGUAGLIANZA
  - TITOLO IV SOLIDARIETÀ
  - TITOLO V CITTADINANZA
  - TITOLO VI GIUSTIZIA

I diritti e le libertà delle persone fisiche

- (75) 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, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo…

Parere 218/14 del WP29:

- …Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria (…).
- In the context referred to above, the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

Misure tecniche e organizzative adeguate…

- 14. In primo luogo, ciò significa che l'articolo 25 non richiede l'attuazione di misure tecniche e organizzative specifiche, bensì che le misure e le garanzie scelte siano specificamente connesse all'attuazione dei principi di protezione dei dati nello specifico trattamento.

- 15. In secondo luogo, **i titolari del trattamento devono essere in grado di dimostrare** che i principi siano stati rispettati.
- 16. Le misure e le garanzie attuate devono conseguire l'effetto auspicato in termini di protezione dei dati e il titolare del trattamento **deve disporre della documentazione relativa alle misure tecniche e organizzative**. A tale scopo, il titolare può definire idonei indicatori chiave di prestazione (ICP/KPI) per dimostrare l'efficacia. Un ICP è un valore misurabile scelto dal titolare che dimostra con quanta efficacia questi riesca a conseguire il suo obiettivo di protezione dei dati. Gli ICP possono essere quantitativi, come la percentuale di falsi positivi o falsi negativi, la riduzione dei reclami, la diminuzione del tempo di risposta quando gli interessati esercitano i loro diritti; o qualitativi, come le valutazioni di prestazione, l'uso di tabelle di classificazione o le valutazioni di esperti. In alternativa agli ICP, i titolari possono dimostrare che l'attuazione dei principi è efficace indicando i criteri alla base della loro valutazione dell'efficacia delle misure e delle garanzie scelte.

Il principio-chiave della *«privacy by design»*, è il garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

Conta non solo ***cosa*** si è fatto ma anche ***perché*** lo si è fatto ed essere sempre in grado *dimostrarlo (accountability)* e la conformità all'*intero regolamento*.

Dobbiamo quindi poter **misurare ex ante** la **reale capacità** delle azioni intraprese **di portare i risultati desiderati.**

Ma per misurare è innanzitutto necessario individuare ***cosa misurare*** *:* quali indicatori usare.

PbD e accountability

LAG INDICATOR

In genere si preferiscono misurare i risultati (***ex-post = lag indicators***), perché sono più facili da valutare, sono precisi ed in genere inconfutabili.

LEAD INDICATOR

Per influenzare il futuro è invece necessario utilizzare un altro tipo di misura, in grado in qualche modo, di anticiparlo (***ex-ante = lead indicators)***

La loro adozione può costituire :

- una **evidenza** dell'attività di analisi e verifica messi in atto da chi effettua il trattamento
- un **fattore esimente** nel caso in cui sia inflitta una sanzione pecuniaria per la cui valutazione l'autorità di controllo *tiene conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32*.

Stato dell'arte

→ di tenere conto degli attuali progressi compiuti dalla tecnologia disponibile sul mercato.

→ rimanere sempre aggiornati sulle opportunità e i rischi

- 20. Lo «stato dell'arte» è un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione continuativa nel contesto dei progressi tecnologici. Di fronte a tali progressi, un titolare può riscontrare che una misura in precedenza atta a conferire un livello di protezione adeguato ora non lo è più. Trascurare l'aggiornamento sui progressi tecnologici potrebbe, quindi, comportare una mancata osservanza dell'articolo 25.

Stato dell'arte

- 21. Il criterio dello «stato dell'arte» non si applica esclusivamente alle misure tecnologiche, ma anche a quelle organizzative. La mancanza di misure organizzative adeguate può ridurre o compromettere del tutto l'efficacia di una tecnologia scelta. Possono costituire esempi di misure organizzative l'adozione di politiche interne, la formazione aggiornata in materia di tecnologia, sicurezza e protezione dei dati nonché politiche di gestione e di governance della sicurezza informatica.

Costi di attuazione

- Il costo si riferisce alle risorse in generale, compresi il tempo e le risorse umane.

- 25. Le misure individuate devono pertanto garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure.

Natura, ambito di applicazione, contesto e finalità del trattamento

- 28. In breve, il concetto di natura può essere inteso come le caratteristiche intrinseche del trattamento. L'ambito di applicazione fa riferimento alla dimensione e all'ampiezza del trattamento. Il contesto riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati, mentre la finalità si riferisce agli obiettivi del trattamento.

Rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

- 30. Nell'analizzare i rischi ai fini del rispetto di quanto prevede l'articolo 25, il titolare deve individuare i rischi per i diritti degli interessati associati a una violazione dei principi,

Valutazione del rischio

THREAT OCCURRENCE PROBABILITY	IMPACT LEVEL: Low	Medium	High / Very High
Low		X	
Medium			
High			

Articolo 24

Responsabilità del titolare del trattamento (C74-C78)

1. 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.*

Articolo *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:*

...

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

1.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.*

I diritti e le libertà delle persone fisiche

Articolo 35

Valutazione d'impatto sulla protezione dei dati (C84, C89-C93, C95)

*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.*

7. La valutazione contiene almeno:

...

*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.***

- Una banca tratta i dati non solo dei propri clienti, sia persone fisiche, sia persone giuridiche (quest'ultime non tutelate dal GDPR), ma anche di tutti i soggetti, fra cui persone fisiche, che ricevono o dispongono bonifici nei confronti dei clienti.
- In caso di accesso illegale ai dati di un conto corrente, ad esempio di una clinica che tratta malattie particolari, i dati dei clienti della clinica potrebbero essere diffusi con conseguenze anche gravi (ad esempio discriminazioni).
- Tali soggetti, non necessariamente sono degli interessati, in quanto non è detto che siano soggetti identificabili da parte della banca, ma potrebbero esserlo da parte di altri soggetti

Aspetto temporale

- Al momento di determinare i mezzi del trattamento

- **MEZZI DEL TRATTAMENTO** > variano dagli elementi generali della progettazione di un trattamento fino a quelli dettagliati, e comprendono l'architettura, le procedure, i protocolli, il layout e l'aspetto.

- **MOMENTO** > periodo in cui il titolare decide come verrà effettuato il trattamento e il modo in cui si svolgerà, nonché i meccanismi che verranno impiegati per effettuarlo.

Aspetto temporale

- All'atto del trattamento stesso
- il titolare è tenuto a mantenere su base continuativa la DPbDD

- 39. Tale obbligo **si estende anche ai trattamenti svolti per mezzo di responsabili del trattamento**. Le operazioni di trattamento effettuate dai responsabili dovrebbero essere regolarmente esaminate e valutate dai titolari per garantire che continuino a rispettare i principi e permettano ai titolari di adempiere ai rispettivi obblighi in tale contesto.

Protezione dei dati per impostazione predefinita

- si intende comunemente un **valore preesistente o preselezionato** di un'impostazione configurabile che viene assegnato a un'applicazione informatica, a un programma informatico o a una periferica. Tali impostazioni sono anche chiamate «impostazioni di fabbrica», specialmente per i dispositivi elettronici.
- Ciò significa che, per impostazione predefinita, il titolare non deve raccogliere più dati del necessario, non deve trattare i dati acquisiti oltre quanto sia necessario per le sue finalità né deve conservarli per un periodo superiore a quello necessario. Il requisito di base prevede che la protezione dei dati sia integrata nel trattamento per impostazione predefinita.
- 45. Le stesse considerazioni si applicano alle misure organizzative a sostegno dei trattamenti. Esse dovrebbero essere concepite, sin dall'inizio, per trattare soltanto la quantità minima di dati personali necessari per i trattamenti specifici. Ciò dovrebbe essere tenuto particolarmente in conto nello stabilire le modalità di accesso ai dati da parte di personale con ruoli ed esigenze di accesso diversi.

Quantità dei dati personali raccolti

- 49.I titolari dovrebbero tenere conto sia del volume dei dati personali sia delle tipologie, delle categorie e del livello di dettaglio dei dati personali richiesti per le finalità del trattamento

La portata del trattamento

- 51. I trattamenti effettuati sui dati personali devono limitarsi a quanto è necessario

Il periodo di conservazione

- 52. I dati personali raccolti non devono essere conservati se non sono necessari per la finalità del trattamento e non sussiste altra finalità compatibile né altro fondamento giuridico ai sensi dell'articolo 6, paragrafo 4.
- Se i dati personali non sono più necessari ai fini del trattamento, allora per impostazione predefinita sono cancellati o resi anonimi
- il titolare dovrebbe disporre di procedure sistematiche per la cancellazione o l'anonimizzazione dei dati, integrate nel trattamento

Obbligo di minimizzazione dei dati

GDPR – Art. 5	675/96 – Art. 9
1. I dati personali sono:… d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); 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…	1. I dati personali oggetto di trattamento devono essere:… c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Obbligo di minimizzazione dei dati

Per determinare quindi il tipo di intervento che il Titolare può mettere in atto si devono valutare le seguenti possibilità:

(a) il dato è usato per una sola finalità. Il dato può quindi:

- essere cancellato, se non sussistono impedimenti tecnici, se è stata richiesta la sua cancellazione
- essere cancellato, se non sussistono impedimenti tecnici o reso, ad esempio anonimo, se è terminato il periodo di conservazione per la specifica finalità.

(b) il dato è usato per finalità diverse, ma è presente una sola volta negli archivi; in questo caso il dato non può essere cancellato. Se infatti il tempo di conservazione per la finalità A è di 5 anni e per la finalità B di 10 anni quello che il Titolare dovrà fare non sarà la cancellazione del dato trascorsi i primi 5 anni, ma impedire che lo stesso sia utilizzato per la prima finalità.

(c) il dato è usato per finalità diverse, ma è presente replicato negli archivi per ogni finalità. Può quindi applicarsi quanto descritto al punto (a)

(d) il dato è usato per finalità diverse, ma è presente replicato negli archivi solo per alcune finalità. Devono essere applicate quindi le regole del punto (a) o del punto (b) in funzione delle circostanze.

Accessibilità dei dati

- 55. Il titolare dovrebbe prevedere limitazioni quanto ai soggetti abilitati all'accesso e alla tipologia dell'accesso ai dati personali sulla base di una valutazione della necessità e assicurare che i dati personali siano realmente accessibili a chi ne ha bisogno in caso di necessità, ad esempio in situazioni critiche. I controlli dell'accesso dovrebbero essere effettuati per l'intero flusso di dati durante il trattamento.

Esattezza

Tra gli elementi principali della progettazione e dell'impostazione predefinita, relativi all'esattezza, possono figurare:

- fonte dei dati – le fonti dei dati personali dovrebbero essere affidabili in termini di esattezza dei dati;
- grado di esattezza – ciascun elemento dei dati personali deve essere il più esatto possibile in base alle necessità delle finalità specifiche;
- esattezza misurabile – occorre ridurre il numero di falsi positivi/negativi, per esempio le distorsioni generate nell'ambito delle decisioni automatizzate e dell'intelligenza artificiale;
- verifica – a seconda della natura dei dati, e in relazione alla frequenza delle relative modifiche, il titolare dovrebbe verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi (per esempio rispetto ai requisiti di età);

PRINCIPI

•cancellazione/rettifica – il titolare dovrebbe cancellare o rettificare tempestivamente i dati inesatti e, in particolare, agevolare questa procedura se gli interessati sono o erano minori e successivamente desiderano eliminare i suddetti dati personali;

•evitare la propagazione di errori – i titolari dovrebbero attenuare l'effetto di un errore accumulato nella catena di trattamento;

•accesso – gli interessati dovrebbero ricevere informazioni sui dati personali e disporre di un accesso efficace agli stessi, ai sensi degli articoli da 12 a 15 del RGPD, per controllarne l'esattezza e apportare le rettifiche ove necessario;

•esattezza permanente – i dati personali dovrebbero essere esatti in tutte le fasi del trattamento e nelle fasi critiche dovrebbero essere effettuate verifiche di esattezza;

•aggiornamento – i dati personali sono aggiornati qualora ciò sia necessario per la specifica

finalità;

•progettazione dei dati – impiego di caratteristiche organizzative e tecnologiche di progettazione per ridurre le eventuali inesattezze, per esempio proponendo scelte concise e predeterminate anziché campi a testo libero.

Responsabilizzazione

- 64. Il principio di responsabilizzazione ha natura trasversale: prevede che il titolare risponda della scelta delle misure tecniche e organizzative necessarie.
- 86. Il principio di responsabilizzazione prevede che il titolare sia responsabile della conformità a tutti i principi …e sia in grado di dimostrarla.
- 87. Il titolare deve essere in grado di dimostrare la conformità ai principi; in tal modo può comprovare gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci, dimostrando ad esempio in che modo una determinata misura sia adeguata a garantire efficacemente il principio di limitazione della conservazione.

Responsabilizzazione

(74) ...il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere **in grado di dimostrare** la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure...

(85) ... a meno che il titolare del trattamento **non sia in grado di dimostrare** che, conformemente al principio di responsabilizzazione...

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

...

2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e **in grado di comprovarlo** («**responsabilizzazione**»).

Articolo 24 **Responsabilità del titolare del trattamento**

... il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed **essere in grado di dimostrare**

Articolo 35 **Valutazione d'impatto sulla protezione dei dati**

...

d) ...e **dimostrare la conformità** al presente regolamento...

Implementing accountability - OECD Privacy Framework

(15. A data controller should:

a) Have in place a privacy management programme that:

i. gives effect to these Guidelines for all personal data under its control;

ii. is tailored to the structure, scale, volume and sensitivity of its operations;

iii. provides for appropriate safeguards based on privacy risk assessment;

iv. is integrated into its governance structure and establishes internal oversight mechanisms;

v. includes plans for responding to inquiries and incidents;

vi. is updated in light of ongoing monitoring and periodic assessment;

b) Be prepared to demonstrate its privacy management programme as

appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting

adherence to a code of conduct or similar arrangement giving

binding effect to these Guidelines; and

c) Provide notice, as appropriate, to privacy enforcement authorities or

other relevant authorities where there has been a significant security

breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

How can I demonstrate that I comply? - www.ico.org.uk

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - Data minimisation;
  - Pseudonymisation;
  - Transparency;
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.
- You can also:
- Adhere to approved codes of conduct and/or certification schemes.

Documenter la conformité - www.cnil.fr

Votre dossier devra notamment comporter les éléments suivants

- **La documentation sur vos traitements de données personnelles**
  - le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants),
  - les analyses d'impact sur la protection des données (PIA ; voir étape 4) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes,
  - l'encadrement des transferts de données hors de l'Union européenne (notamment les clauses contractuelles types ou les BCR).
- **L'information des personnes**
  - les mentions d'information,
  - les modèles de recueil du consentement des personnes concernées,
  - les procédures mises en place pour l'exercice des droits des personnes.
- **Les contrats qui définissent les rôles et les responsabilités des acteurs**
  - les contrats avec les sous-traitants,
  - les procédures internes en cas de violations de données,
  - les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Documentare la conformità

Appendice D - Elenco documenti

OBBLIGATORI: Ben definiti ed il cui contenuto è specificatamente declinato

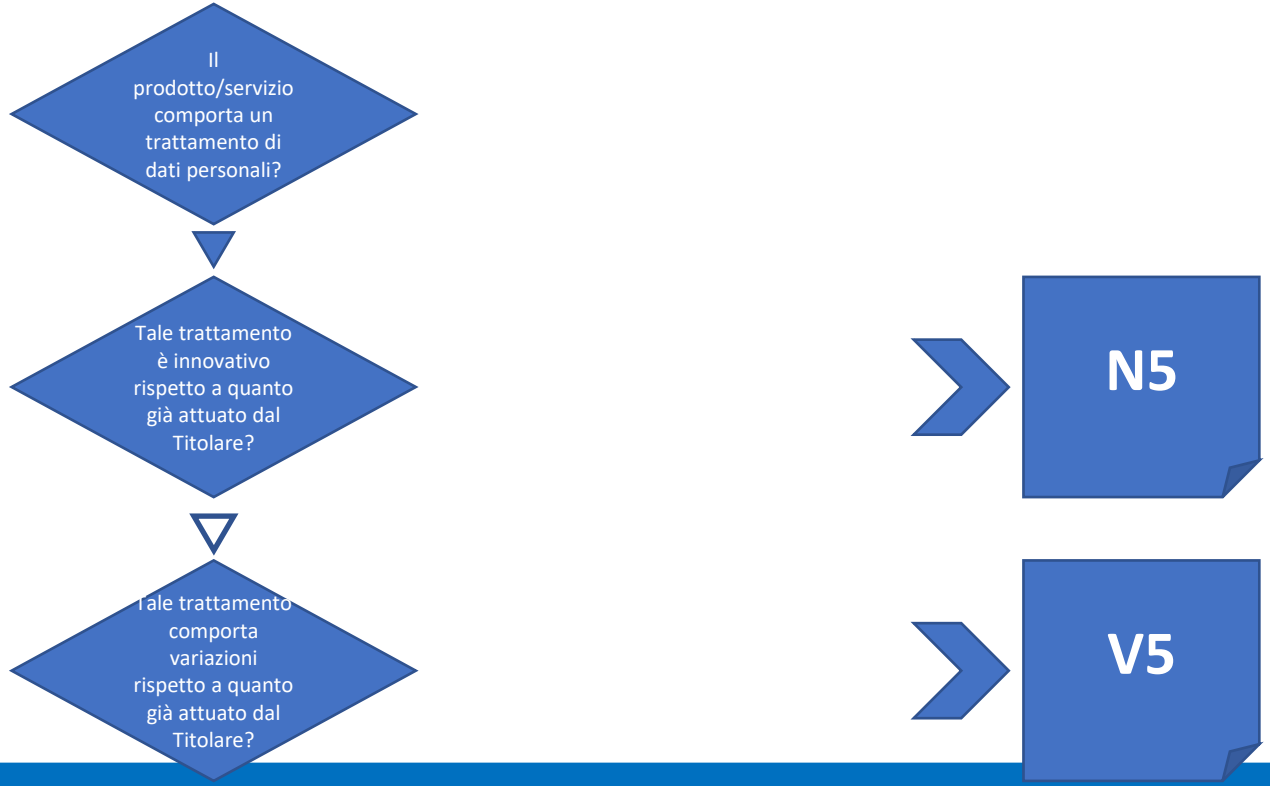
- informative
- formula del consenso
- contratti di designazione dei responsabili
- contratti di designazione dei sub responsabili
- contratti o altri atti per contitolarità, rappresentanza…
- designazione amministratori di sistema
- designazione del DPO
- istruzioni per i soggetti che operano sotto l'autorità del Titolare o del Responsabile
- regolamentazione del trasferimento dei dati all'estero
- registri delle attività di trattamento
- registro delle violazioni
- notifica di violazione all'Autorità Garante
- comunicazione di violazione agli interessati
- DPIA
- Norme vincolanti d'impresa
- Comunicazione preventiva all'Autorità Garante (art. 36)

Per quanto il rispetto dell'articolo 25.1 sia molto impegnativo, non è esaustivo di tutti quelli che sono i requisiti previsti dalla normativa.

È quindi utile, per garantirne il rispetto, analizzare, nel caso di nuovi trattamenti, qualunque altro adempimento previsto dalla stessa.

Al riguardo è utile effettuare una schematizzazione come quella riportata nel seguito, che ha carattere puramente indicativo

N4 Nuovo servizio/prodotto



N5 Nuovo trattamento *(es. finalità, interessati, dati trattati)*

Definire la finalità del trattamento
Individuare i soggetti interessati
Definire la base giuridica del trattamento
Individuare gli strumenti utilizzati per effettuare il trattamento
Individuare i soggetti interni ed esterni che partecipano al trattamento
Individuare i soggetti ai quali sono comunicati i dati e la loro collocazione
In presenza di trasferimento all'estero individuare le garanzie individuate
Definire i tempi di conservazione dei dati

Censire il trattamento nel Registro delle attività di trattamento → A1

Effettuare le analisi del rischio previste dagli artt. 24, 25, 32 → A3

Nuove informative/variazioni informative → A2

Variazione ruoli → R

Implementazioni tecniche ed organizzative

Grazie per l’attenzione

giancarlo.butti@promo.it
gbutti@clusit.it