IL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (REGOLAMENTO UE 2016/679)

Prof. Stefano Troiano

Ordinario di diritto privato
Università degli Studi di Verona - Dipartimento di Scienze Giuridiche

Natura, finalità e caratteristiche del GPDR

- Strumento di uniformazione dotato di diretta applicabilità → teso a eliminare la frammentazione e rafforzare la fiducia nelle transazioni elettroniche nel mercato interno
- Struttura: 99 articoli ripartiti in 11 Capi, preceduti da 173 considerando
  - Capo I – Disposizioni generali
  - Capo II – Principi
  - Capo III – Diritti dell'interessato
  - Capo IV – Titolare del trattamento e responsabile del trattamento
  - Capo V – Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
  - Capo VI – Autorità di controllo indipendenti
  - Capo VII – Cooperazione e coerenza
  - Capo VIII – Mezzi di ricorso, responsabilità e sanzioni
  - Capo IX – Disposizioni relative a specifiche situazioni di trattamento
  - Capo X – Atti delegati e atti di esecuzione
  - Capo XI – Disposizioni finali
- Un codice europeo dei dati personali? un testo unico? Un restatement?

1

Principi

- Nessun cambiamento rivoluzionario: si riafferma il diritto alla protezione dei dati personali come base giuridica (principale).
- art. 1 (2): « *Il presente Regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali* »
- Articolo 5: liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

2

Il diritto alla protezione dei dati personali: evoluzione storica

- dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- l. 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
- art. 1 del d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, che recita: "chiunque ha diritto alla protezione dei dati personali che lo riguardano"
- Art. 8 Carta dei diritti fondamentali dell'Unione europea

3

L'oggetto del diritto: i "dati personali"

- costituisce 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"
- Sono, invece, esclusi dall'ambito di applicazione della normativa i dati o le informazioni anonime, definite dal considerando 26 come "*informazioni che non si riferiscono a una persona fisica identificata o identificabile*" o "*dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato*" (e, dalla legge italiana, "*il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile*").

4

Distinzione rispetto al diritto alla riservatezza

- diritto alla protezione dei dati personali → diritto di un soggetto di controllare l'insieme delle informazioni che a questi si riferiscono / libertà positiva di esercitare un controllo sul flusso delle proprie informazioni
- diritto alla riservatezza → diritto di escludere altri dalla conoscenza di vicende strettamente personali e familiari (diritto a contenuto negativo, 'right to be let alone') - Convenzione di Strasburgo e art. 7 Carta dei diritti fondamentali dell'Unione europea

5

Le principali novità del GPDR

- Generale cambiamento di prospettiva: dalla mera protezione dei dati alla regolazione e alla *compliance* (approccio dinamico)
- Novità di natura sostanziale:
  - ampliamento dell'ambito di applicazione
  - nuove definizioni sia oggettive sia soggettive
  - parziale rivisitazione della disciplina del consenso
  - nuovi diritti o diritti parzialmente rivisitati
  - nuova disciplina della responsabilità e delle sanzioni
  - nuovo "risk- and compliance-based approach"
- Novità di natura istituzionale, organizzativa e procedurale:
  - poteri delle autorità
  - sanzioni
  - Rete di autorità
  - Legittimazione ad agire, ecc.

6

Ampliamento del campo di applicazione

- Si introduce il principio in base al quale le regole sulla protezione dei dati personali si applicano a prescindere dal criterio formale della territorialità del titolare del trattamento, ossia si applicano in base a un **criterio sostanziale** di sfruttamento dei dati dei soggetti interessati anche attraverso l'uso di Internet.

Art. 3 – Ambito di applicazione territoriale

- 1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
- 2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
  - a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
  - b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
- 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

7

Definizioni: le novità

Scompaiono alcune definizioni, ne vengono riviste altre già esistenti e vengono altresì introdotte nuove definizioni (Art. 4). Ad es.:

- n. 4) **"profilazione"**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- n. 5) **"pseudonimizzazione"**: "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" (nuova).
- n. 12) **"violazione dei dati personali"**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- n. 14) **"dati biometrici"**: "i 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" (nuova)

8

Definizioni: i soggetti

- Art. 4, n. 7 - **Titolare del trattamento** / "Controller" (DC)
  - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo 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;
- Art. 4, n. 8 - **Responsabile del trattamento** / "Processor" (DP)
  - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
- Art. 37 ss.
  - **Responsabile della protezione dei dati** - RPD / "Data Protection Officer" (DPO)

Scompare, ma solo formalmente, la figura dell'"incaricato del trattamento", di fatto però regolata *sub* art. 29

9

Criteri di liceità del trattamento: il consenso

- Criterio principale di liceità rimane il consenso dell'interessato
  - N.B. Non è però l'unico: v. art. 6
- Il consenso, inteso (art. 4, n. 11) come qualsiasi manifestazione di assenso dell'interessato, deve essere libero, specifico, informato e inequivocabile, cioè espresso mediante dichiarazione o azione positiva inequivocabile (non può mai essere desunto dal silenzio o da un comportamento inattivo: v. considerando 32)
  - N.B. in tre casi, però, il consenso deve essere esplicito
- Il consenso non dovrebbe costituire il presupposto per un valido trattamento qualora vi sia un "*evidente squilibrio tra interessato e titolare del trattamento*", soprattutto nei casi in cui quest'ultima sia un'autorità pubblica o comunque si possa presumere che il consenso non si sia liberamente formato (Considerando 43)
- Il consenso è liberamente revocabile (art. 7, par. 3)

10

Criteri di liceità del trattamento: l'informativa

- L'informativa dovrà contenere più elementi rispetto al passato (ad es., intenzione di trasferire i dati all'estero)
- Si prevede, inoltre, un generale dovere di trasparenza: Le informazioni dovranno essere coincise, facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro (ad esempio, con l'uso di simboli grafici, con libero accesso via web, ecc.);
- inoltre il Regolamento prevede due tipologie di informativa, che si distinguono a seconda che i dati vengano raccolti presso l'interessato (art. 13) o non siano stati ottenuti presso l'interessato (art. 14).

11

La prova del consenso

- È innovativa la previsione introdotta dall'art. 7, par. 1: "qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali".
- si pone in capo al titolare un vero e proprio onere della prova sulla raccolta del consenso
- Per converso non è necessario che il consenso sia documentato per iscritto (v. invece art. 23, co. 3 cod. privacy)

12

Il consenso del minore

- Art. 8, comma 1:
  - qualora l'interessato abbia espresso il suo consenso "per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni".
  - "Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale"

13

I Big Data

- il consenso dell'interessato non è necessario quando i dati, raccolti per un determinata finalità, sono utilizzati a 'scopo di ricerca statistica'[18] (Articolo 5.1.b: «... *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 ..*»).
- il Regolamento ha altresì adottato disposizioni atte a contenere o quanto meno arginare gli effetti negativi delle decisioni automatiche a seguito di profilazione derivanti da Big Data (art. 22).

14

Altre novità: foro competente, responsabilità civile

- Mutano le disposizioni sul foro competente, con la previsione di più fori alternativi
  - art. 79, comma 2
- Muta il regime di responsabilità civile **(Art. 82)**
  - 1. 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.
  - 2. Un **titolare del trattamento** coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un **responsabile del trattamento** risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
  - 3. Il 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**.

QUESTIONI:
- Qual è l'interesse leso (v. anche le esemplificazioni di cui al considerando 75)?
- Qual è il danno risarcibile?
- Quando risponde il responsabile del trattamento?
- Quando si ha esonero dalla responsabilità?

15

Segue: le sanzioni

- Estremamente elevate sono le sanzioni amministrative che possono giungere fino al 4% del fatturato,
- In particolare:
  - SANZIONI AMMINISTRATIVE PECUNIARIE (art. 83), in funzione delle circostanze di ogni singolo caso, effettive, proporzionate e dissuasive; molto più pesanti rispetto al passato.
  - sanzioni amministrative pecuniarie fino a 10.000.000 (dieci milioni) di EURO o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nel caso delle infrazioni di cui all'articolo 83, paragrafo 4), lettere a), b) e c); sanzioni amministrative pecuniarie fino a 20.000.000 (venti milioni) di EURO o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nel caso delle infrazioni di cui all'articolo 83, paragrafo 5), lettere a), b), c), d) ed e).
  - E' espressamente vietato il cumulo materiale delle sanzioni amministrative (art. 83, paragrafo 3) nel caso in cui vengano violate varie disposizione del regolamento, con comminazione dell'importo più elevato tra le sanzioni amministrative pecuniarie.

16

Segue: i vecchi e i nuovi diritti

- Sono confermati i diritti dell'interessato all'accesso, alla rettifica e all'opposizione al trattamento dei propri dati
- Se ne aggiungono di nuovi (o parzialmente nuovi):
  - diritto all'"oblio" (art. 17, comma 2):
    - il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, "tenendo conto della tecnologia disponibile e dei costi di attuazione adotta misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali"
  - diritto alla portabilità dei dati (art. 20),
    - ossia "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: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati"

17

La principale novità: il principio di *accountability*

- Accountability = "responsabilità" ma anche "prova della responsabilità".
  - Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi
  - È un modo di **creare una procedura** (tipico approccio anglosassone) al fine di:

    (a) ***garantire* l'osservanza** e

    (b) ***dimostrare* che il trattamento è stato effettuato conformemente** al Regolamento
- l'accountability è un meccanismo a due livelli:
  - attuazione di misure e/o procedure, e conservazione delle relative prove
  - sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime

18

Gli obblighi del titolare e del respons. del trattamento

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

→ **e v. anche Art. 25:** *Privacy by design* e *Privacy by default*

- **Articolo 28 – Il responsabile del trattamento**

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

19

Segue: l'obbligo di tenuta dei registri

- **Articolo 30 – I registri delle attività di trattamento**

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: (…)
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: (…)
3. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

20

Segue: Certificazione

- Strettamente collegata al principio di *accountability* è la previsione di meccanismi di certificazione della conformità delle misure adottate alla legge vigente
  - V., ad es., art. 24, comma 3: "L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento".
  - oppure (con riguardo alle misure di sicurezza) art. 32, comma 3: "l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo".

Accreditamento degli organismi di certificazione secondo la norma UNI CEI EN ISO/IEC 17065:2012 integrata però da requisiti aggiuntivi ancora da definire (v. Comunicazione Garante 18.07.2017)

21

Corollario: il nuovo *risk-based approach*

- Nuovo approccio alla regolamentazione del trattamento dei dati personali incentrato sull'analisi e gestione del rischio → principio di c.d. *accountability*
- Modello di responsabilità volto alla prevenzione del danno
  - Le nuove disposizioni rafforzano dunque la responsabilità dei titolari del trattamento che, a norma dell'art. 24, reg. UE 2016/679, rispondono per la mancata attuazione delle "misure tecniche e organizzative" volte ad affrontare i rischi di cui al Regolamento (v. anche art. 83, par. 4, reg. UE 2016/679)
- Passaggio da una dimensione individuale del danno a una dimensione collettiva

22

Il rischio rilevante

- Nozione estesa: rischio di essere profilati, di vedere le proprie informazioni condivise con terzi, di essere monitorati a fini commerciali e quant'altro
  - Tutte queste conseguenze non sono correlate a forme di trattamento di per sé illecite, anzi solitamente sono legittimate dall'accettazione da parte dell'interessato
- Nozione ristretta (ma comunque ampia): danni "materiali o non materiali" che possono derivare dal pregiudizio dei "diritti e libertà delle persone fisiche" (Cfr. art. 24 (1) Reg. UE e 75° considerando)
- cause d'illiceità del trattamento

23

Obbligo di adottare misure di sicurezza adeguate al rischio

- Art. 32: obbligo di mettere in atto "le misure tecniche e organizzative adeguate per garantire un livello di sicurezza [del trattamento] adeguato al rischio (…)"
  - Scompaiono le c.d. "misure minime di sicurezza"

→ Sicurezza come concetto **dinamico** e **relazionale**

→ Continuo monitoraggio:
  - Occorre una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di policy interne e quindi un'attività di monitoraggio continuo

24

La valutazione d'impatto (DPIA)

- L'*accountability* richiede tre diverse fasi: a) l'analisi del processo, prodotto o attività, b) la valutazione del rischio, c) la definizione delle misure idonee ad escludere o mitigare il rischio
- A sua volta, l'analisi del rischio si articola in più livelli:
  - Primo livello: Prima valutazione del rischio generica e non formalizzata (artt. 24 e 35, par. 1): valutazione dei trattamenti e dei rischi, della necessità dei trattamenti stessi e infine individuazione di misure di sicurezza adeguate
  - Secondo livello: valutazione formale d'impatto sulla protezione dei dati
  - Terzo livello: consultazione preventiva
- Approccio basato sui metodi privacy by design e privacy by default, di cui all'art. 25, che prevedono specificamente l'adozione di misure di pseudonimizzazione e minimizzazione del trattamento dei dati, nonché di protezione dei dati con riguardo all'accesso
  - Problema: Impiego di numerosi concetti giuridici indefiniti

25

(segue) la valutazione d'impatto: presupposti

- L'Art. 35 e le relative *Guidelines* del 4 aprile 2017 del WP29 :
  - La DPIA è obbligatoria solo "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" (Art. 35, par. 1) ("…is likely to result in a high risk to the rights and freedoms of natural persons")
    - **N.B.** In caso di dubbio, il Gruppo 29 consiglia di effettuare comunque la DPIA.
  - Vi sono però casi tipici (art. 35, par. 3) in cui il grado elevato del rischio è presunto e la valutazione obbligatoria, "in particolare" in caso di:
    - 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;
    - 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
    - la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

26

(segue) categorie particolari di dati

- L'art. 35, par. 3, identifica dunque una serie di fattispecie in cui la valutazione d'impatto è richiesta "in particolare" e, tra queste, figura l'ipotesi di trattamento "su larga scala" delle categorie particolari di dati di cui all'art. 9, par. 1.
- resta però oscuro è il significato della (infelice) locuzione "su larga scala",
  - Cfr. 91° considerando
- È una lista aperta e non esaustiva. L'Autorità redige un elenco pubblico (Art. 35, par. 4). Il Gruppo 29 ha indicato alcuni criteri di massima (p. 7 ss.), basati anche sui Considerando 71, 75 e 91
  - Quando la DPIA **non** è richiesta? (v. esempi del WP29, p. 11)
  - Si applica a operazioni di trattamento già esistenti?
    - Si applica a quelle iniziate dopo il 25 maggio 2018 oppure a quelle iniziate prima ma modificate in modo significativo dopo quella data.

27

(segue) la valutazione d'impatto (DPIA): quando?

- Il processo di analisi dei rischi va periodicamente rivisto
  - In particolare, quanto ci sia un cambiamento del rischio che l'operazione di trattamento presenta (Art. 35(11)).
- Quando va effettuata una DPIA?
  - La DPIA deve essere effettuata "prima del trattamento" (Artt. 35(1) e 35(10), considerando 90 e 93), in conformità ai principi "protection by design" e "protection by default" (Art. 25 e considerando 78).
    - In alcuni casi la DPIA sarà un processo continuo (on-going process), es. quando l'operazione di trattamento è dinamica e soggetto a cambiamenti continui.

28

Segue: la valutazione d'impatto (DPIA): chi?

- Chi la compie?
  - Il data controller (titolare del trattamento) insieme al DPO e al data processor (responsabile del trattamento). In particolare:
    - Il titolare del trattamento deve assicurare che la DPIA sia effettuata (Art. 35(2)). In concreto la DPIA può essere compiuta anche da altri, interni o esterni all'organizzazione, ma chi ne risponde è sempre il titolare.
    - Il titolare deve anche chiedere consiglio al Data Protection Officer (DPO), ove ne sia nominato uno (Art. 35(2)) e la consulenza di quest'ultimo e le decisioni prese devono essere documentati nella DPIA. Il DPO deve anche monitorare l'esecuzione della DPIA (Art. 39(1)(c)).
    - Se il trattamento è in tutto o in parte eseguito da un responsabile del trattamento (data processor), questi deve assistere il titolare nell'effettuare la DPIA e fornire ogni necessaria informazione.
    - Il titolare deve raccogliere i pareri delle persone interessate dai dati o dei loro rappresentanti (Article 35(9)), "quando opportuno".

29

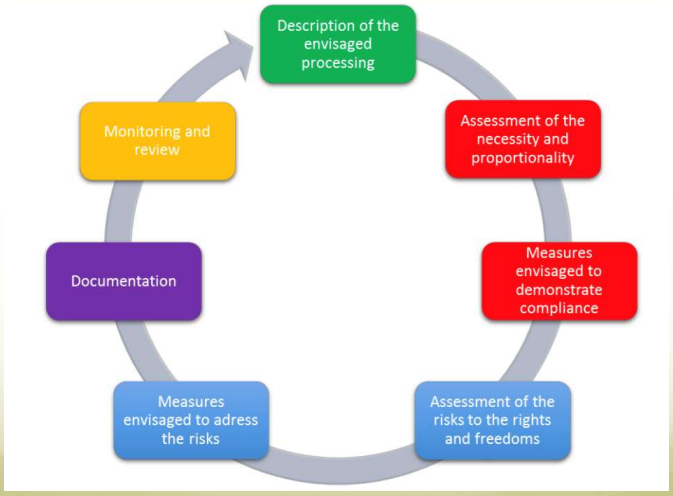
La DPIA: metodologia

- Quale metodologia seguire nella DPIA?
- Il GDPR requisiti minimi di una DPIA (Art. 35(7), e considerando 84 e 90):
  - - "una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento";
  - - "una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità";
  - - "una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1";
  - - "le misure previste per:
    - affrontare i rischi;
    - dimostrare la conformità al presente regolamento"

30

La DPIA come processo

- La DPIA si svolge secondo un processo iterativo (fonte: WP29):



31

La DPIA: altri profili

- La DPIA deve essere resa pubblica?
  - Il GDPR non richiede che la DPIA sia resa pubblica.
  - La scelta di pubblicarla è rimessa al titolare del trattamento.
  - Il Gruppo Art. 29 ne consiglia, però, la pubblicazione, eventualmente anche solo parziale, al fine di aumentare la fiducia nelle operazioni di trattamento effettuate dal titolare e dimostrare la accountability e la trasparenza del medesimo.
  - N.B.: La pubblicazione è, comunque, obbligatoria in caso di preventiva consultazione dell'Autorità (Art. 36(3)(e)).

32

Consultazione preventiva

- Nei casi in cui è stata effettuata un'analisi formale dei rischi ai sensi dell'art. 35, reg. UE 2016/379 e la stessa evidenzi un rischio elevato in assenza dell'adozione delle opportune misure di mitigazione od eliminazione del rischio, il titolare del trattamento è tenuto alla consultazione preventiva dell'autorità di controllo
- modello simil-autorizzatorio
- Conseguenze della consultazione: tre diversi scenari

33

Segue: la consultaz. prev.

In particolare:

- Il data controller ha la responsabilità di valutare i rischi per i diritti e le libertà dei titolari dei data e identificare le misure necessari per ridurre questi rischi ad un livello accettabile (Article 35(7)).
  - Es. storage of personal data on laptop computers with appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) in addition to existing policies (notice, consent, right of access, right to object, etc.). Qui il titolare ha controllato i rischi e non è necessario dunque procedere alla consultazione preventiva.
- La consultazione preventiva è invece necessaria nei casi in cui i rischi identificati non possono essere gestiti in modo adeguato dal titolare del trattamento, ossia **quando i rischi residui rimangono inaccettabilmente elevati** (unacceptable high residual risk)**.**
  - Es: where the data subjects may encounter significant, or irreversible, consequences, which they may not overcome, and/or when it seems obvious that the risk will occur. Whenever the data controller cannot find sufficient measures (i.e. when the residual risks are still high), consultation with the supervisory authority will be necessary.
- La consultazione preventiva è inoltre necessaria nei casi indicati dall'art. 36(5):
  - "il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

34

La DPIA in sintesi, secondo il Gruppo ex Art. 29

- Se si prevede come probabile un elevato rischio nel trattamento il titolare deve:
  - scegliere una metodologia di DPIA che soddisfi i criteri di cui all'**Allegato 2** (alle Guidelines), o specificare e mettere in atto un processo sistematico di DPIA che:
    - sia conforme ai criteri di cui all'Allegato 2;
    - sia integrato in "existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture";
    - coinvolga i soggetti interessati e ne definisca le responsibilità in modo chiaro (titolare, DPO, persone interessate o loro rappresentanti, "business, technical services, processors, information security officer", ecc.);
  - fornisca il report della DPIA alla competente Autorità di controllo, quando ciò sia richiesto;
  - consulti l'Autorità di controllo quando non sia riuscito a individuare misure sufficienti per mitigare gli elevati rischi rilevati;
  - riveda periodicamente la DPIA e il trattamento a cui essa si riferisce, almeno quando viene a modificarsi il rischio creato dal trattamento;
  - documenti le decisioni assunte.

35

All. n. 2
Guidelines WP29

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)).

Il *Data Protection Officer:* cenni

- Il DPO (Responsabile della protezione dei dati) è il soggetto incaricato di vigilare sul rispetto della normativa in materia di privacy
- Il DPO funge inoltre da punto di contatto con l'autorità di controllo
- È una figura professionale obbligatoria in alcuni casi (es.: per autorità o organismi pubblici, o qualora l'impresa sia di grandi dimensioni o operi trattamenti di dati personali su larga scala)
- deve essere tempestivamente coinvolto in tutte le questioni riguardanti il trattamento di dati personali ed esprimere un parere sulle valutazioni di impatto e cooperare con le autorità di controllo di impatto (art. 38)
- gode di una certa indipendenza e riferisce direttamente al titolare del trattamento (art. 38).

37

Codici di condotta

- Viene promossa l'elaborazione di "CODICI DI CONDOTTA" (artt. 40 e 41) destinati a contribuire alla corretta applicazione del nuovo Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.
- Inoltre, vengono incentivati i processi di "CERTIFICAZIONE" (artt. 42 e 43) o l'acquisizione di "MARCHI" o "BOLLINI" che garantiscano la correttezza e serietà del trattamento

38

Novità relative all'assetto istituzionale

- Modello di regolazione per la protezione dei dati personali basato su una forma ibrida di **enforced self-regulation**
- Ovvero, in sintesi: le autorità di regolazione hanno la responsabilità di vigilare su sistemi di controllo e gestione dei rischi predisposti autonomamente dai soggetti regolati, piuttosto che intervenire direttamente con misure puntuali

39

Parziale riassetto delle Autorità di controllo

- Alle autorità di controllo sono riconosciuti poteri di regolazione tra cui poteri ispettivi, correttivi sanzionatori (questi ultimi in misura molto più ampia del passato)
- al fine di evitare la frammentazione nazionale delle regole sulla protezione dei dati personali, il Regolamento introduce non solo delle procedure di coordinamento tra le autorità di controllo indipendenti dei vari paesi dell'Unione (c.d. "meccanismo di coerenza"), …

40

Comitato Europeo per la Protezione dei Dati Personali (EDPB)

- …ma anche un meccanismo di risoluzione delle controversie generate da pareri o decisioni divergenti
  - → a tal fine viene creato un Comitato *ad hoc* (EDPB) dotato di poteri vincolanti.
- Il Comitato (EDPB) è composto dai rappresentanti delle autorità di controllo nazionali e dal Garante Europeo dei Dati Personali (EDPS)
- L'EDPS fornisce al comitato il Segretariato
- La Commissione partecipa ai lavori con il ruolo di osservatore senza voto

41