Privacy, GDPR e Data Breach

Laboratorio di pratica professionale sulla privacy
Come impostare l'organizzazione privacy

Avv. Andrea Lisi

Digital&Law Department - Studio Legale Lisi

Presidente ANORC Professioni

3 ottobre 2019

ANORC
Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale

ANORC Professioni

A.I.F.A.G. Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica

Digital & Law Department

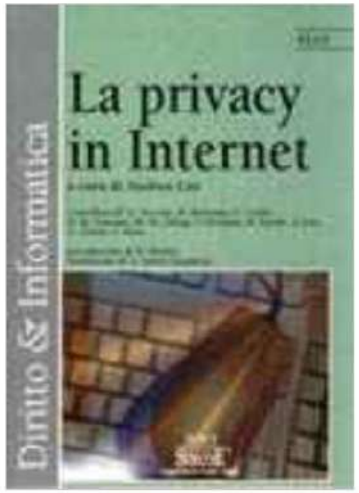
Coalizione dei conservatori accreditati • ANORC • AIFAG

KnowIT

d&l net

il Fatto Quotidiano.it
Non riceve alcun finanziamento pubblico

L'HUFFINGTON POST
IN COLLABORAZIONE CON IL Gruppo Espresso



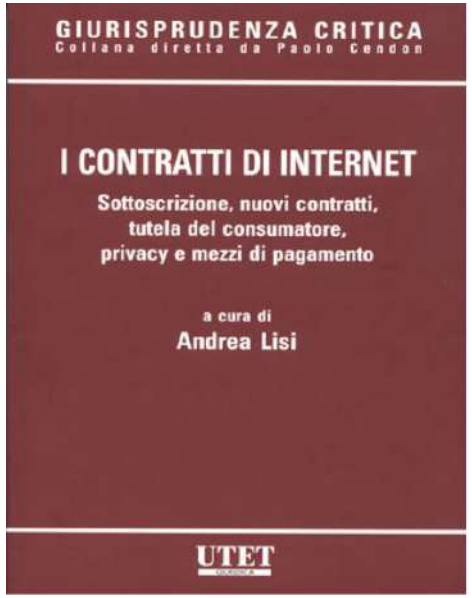
La privacy in Internet

Autori **A. Lisi**

Anno Edizione: **2003**
Formato: **13 x 19**
Pagine: **272**

Codice: **41/25**
Isbn: **9788824490153**

Prezzo: **€ 15,00**



Internet: profili giuridici e opportunità di mercato

di Andrea Lisi edito da Maggioli Editore, 2002

Attualmente l'articolo è fuori catalogo

Informazioni bibliografiche

Titolo del Libro: Internet: profili giuridici e opportunità di mercato
Collana: **Legale**
Genere: **Diritto**
ISBN-10: 8838721610

Autore : **Andrea Lisi**
Editore: **Maggioli Editore**
Data di Pubblicazione: 2002
Pagine: 436
ISBN-13: **9788838721618**

Pubblica amministrazione e privacy. Istruzioni

di Andrea Lisi Federica Bertoni edito da CieRre, 2006

Disponibilità incerta

Informazioni bibliografiche del Libro

Titolo del Libro: Pubblica amministrazione e privacy. Istruzioni per l'uso
Data di Pubblicazione: 2006
Argomenti : **Privacy Amministrazione pubblica**
ISBN-13: **9788871377018**

Autori : **Andrea Lisi Federica Bertoni**
Editore: **CieRre**
Genere: **diritto**
Pagine: 347
ISBN-10: 887137701X

Il negozio telematico. I profili giuridici di un e-shop

di Andrea Lisi edito da Halley Editrice, 2007

Il negozio telematico. I profili giuridici di un e-shop: Con l'informatica e Internet si è potuto prescindere per la prima volta dal supporto cartaceo nello scambio di informazioni e comunicazioni a distanza, passando alle novità e alle comodità della trasmissione e conservazione della documentazione elettronica. Il testo si propone, così, di rendere comprensibile a tutti la materia e di fornire le risposte per capire come è regolamentato lo spazio commerciale telematico e quali sono le regole giuridiche per la realizzazione di un e-shop. L'opera affronta le seguenti tematiche: l' e-commerce nei world wide web: profili giuridici; i contratti informatici e telematici nel mercato digitale; la tutela dei consumatore nei contratti B2C; i contratti B2B e l'e-marketplace; la tutela della privacy nei contratti on-line; i sistemi di e-payment; le problematiche nazionali di Internet. Conclude il libro un'esaustiva appendice normativa e giurisprudenziale.

Attualmente l'articolo è fuori catalogo


PROFESSIONISTA
DELLA PRIVACY
ANORC
Professioni
2019
Andrea LISI
EXPERT
Tessera n°13
L'iscrizione ad ANORC Professioni è da intendersi quale attestazione di qualità e di qualificazione professionale dei servizi prestati dall'associato conforme ai requisiti previsti dagli articoli 4, 7, 8 della Legge 4/2013 (Disposizioni in materia di professioni non organizzate in ordini o collegi).
Il presente tesserino professionale è rilasciato il 16/01/2019 e firmato digitalmente dalla Direzione

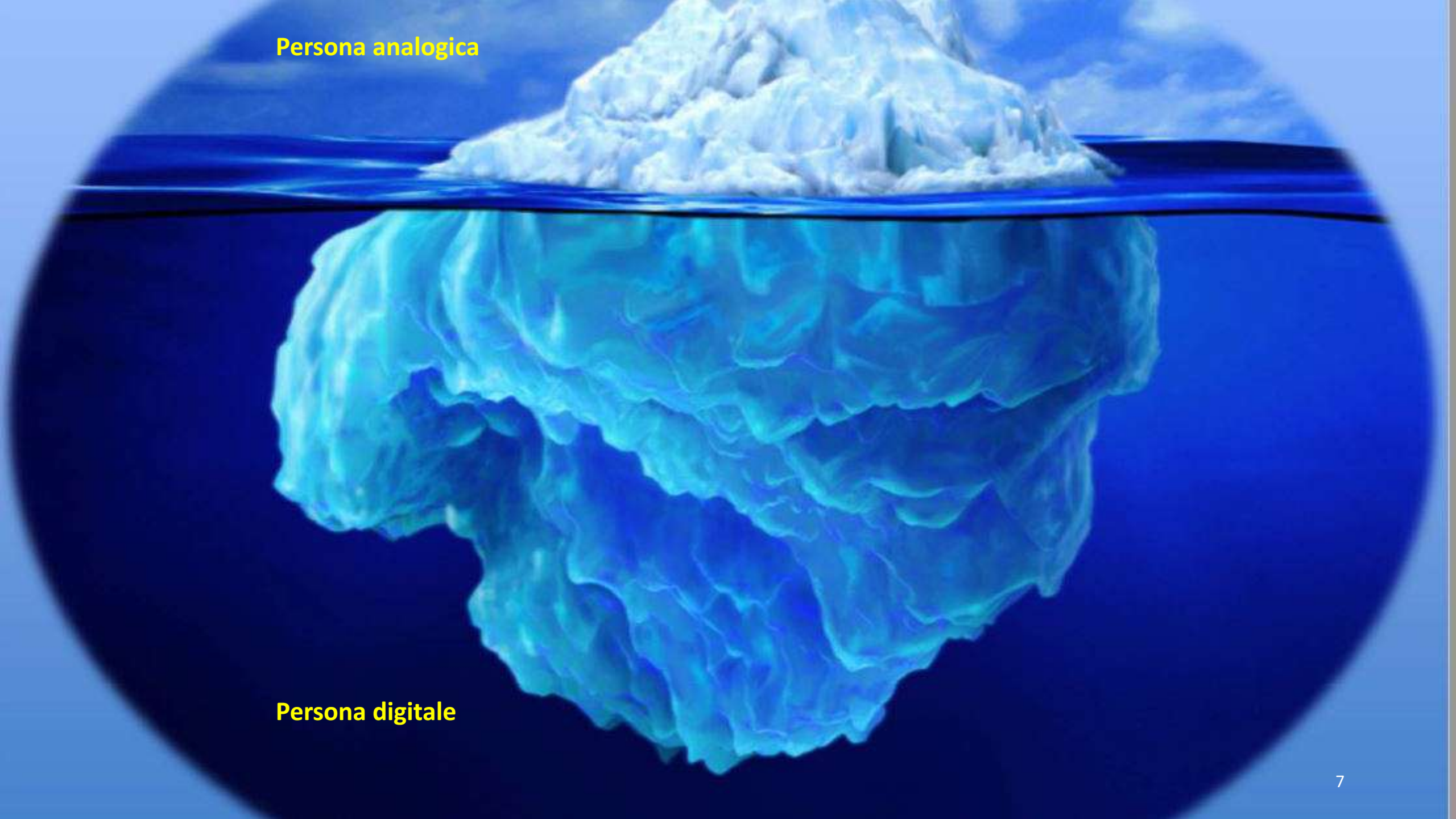

PROFESSIONISTA DELLA
DIGITALIZZAZIONE
ANORC
Professioni
2019
Andrea Lisi
EXPERT
Tessera n° 26
L'iscrizione ad ANORC Professioni è da intendersi quale attestazione di qualità e di qualificazione professionale dei servizi prestati dall'associato conforme ai requisiti previsti dagli articoli 4, 7, 8 della Legge 4/2013 (Disposizioni in materia di professioni non organizzate in ordini o collegi).
Il presente tesserino professionale è rilasciato il 16/01/2019 e firmato digitalmente dalla Direzione.

PREMESSE CONCETTUALI

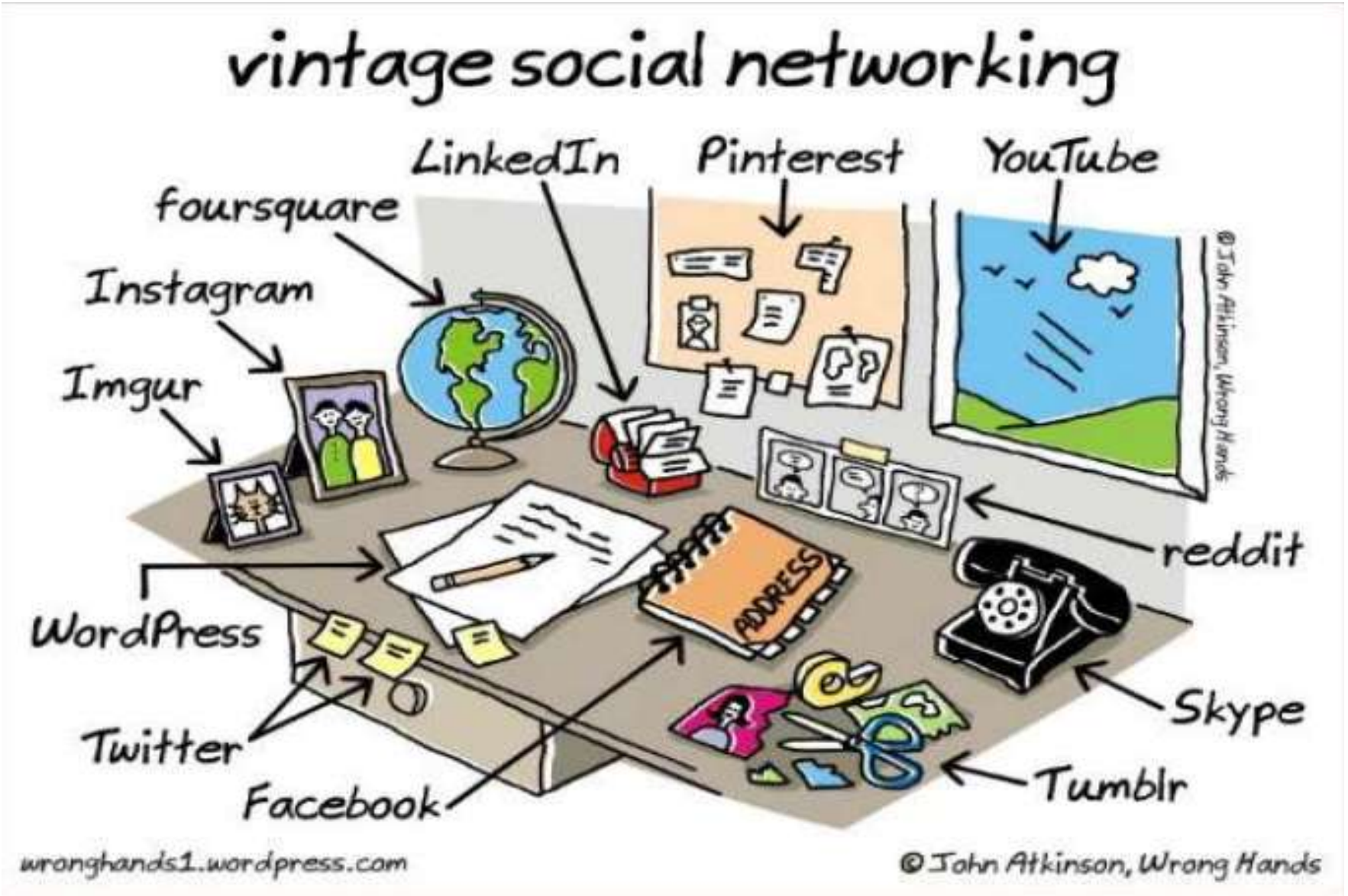
Giovanni Buttarelli

- *L'attuale ecosistema digitale si fonda sullo sfruttamento intensivo ed indiscriminato delle informazioni e dei dati personali. Nel corso di poco più di un decennio, la struttura dei mercati è andata convergendo verso situazioni di quasi-monopolio, decretando l'accrescimento esponenziale del potere di mercato di pochi, ma potentissimi, attori privati. Il risultato è la concentrazione del potere di controllo dei flussi d'informazione nelle mani dei giganti del tech, circostanza che facilita il consolidamento di un modello di business basato sulla profilazione e finanche manipolazione delle persone.*

- *Si rende a tal proposito necessario un ripensamento strutturale del modello di business prevalente. Si impone, inoltre, un intervento coordinato delle autorità della protezione dei dati, della protezione dei consumatori e della concorrenza, che tenga conto delle sinergie e sfide comuni alle diverse aree di regolazione.*


Persona analogica
Persona digitale


Abbiamo davvero bisogno di nativi digitali?


vintage social networking
LinkedIn
Pinterest
YouTube
foursquare
Instagram
Imgur
reddit
WordPress
Twitter
Facebook
Skype
Tumblr
ADDRESS
wronghands1.wordpress.com
© John Atkinson, Wrong Hands


E la privacy che fine ha fatto?

BIG DATA

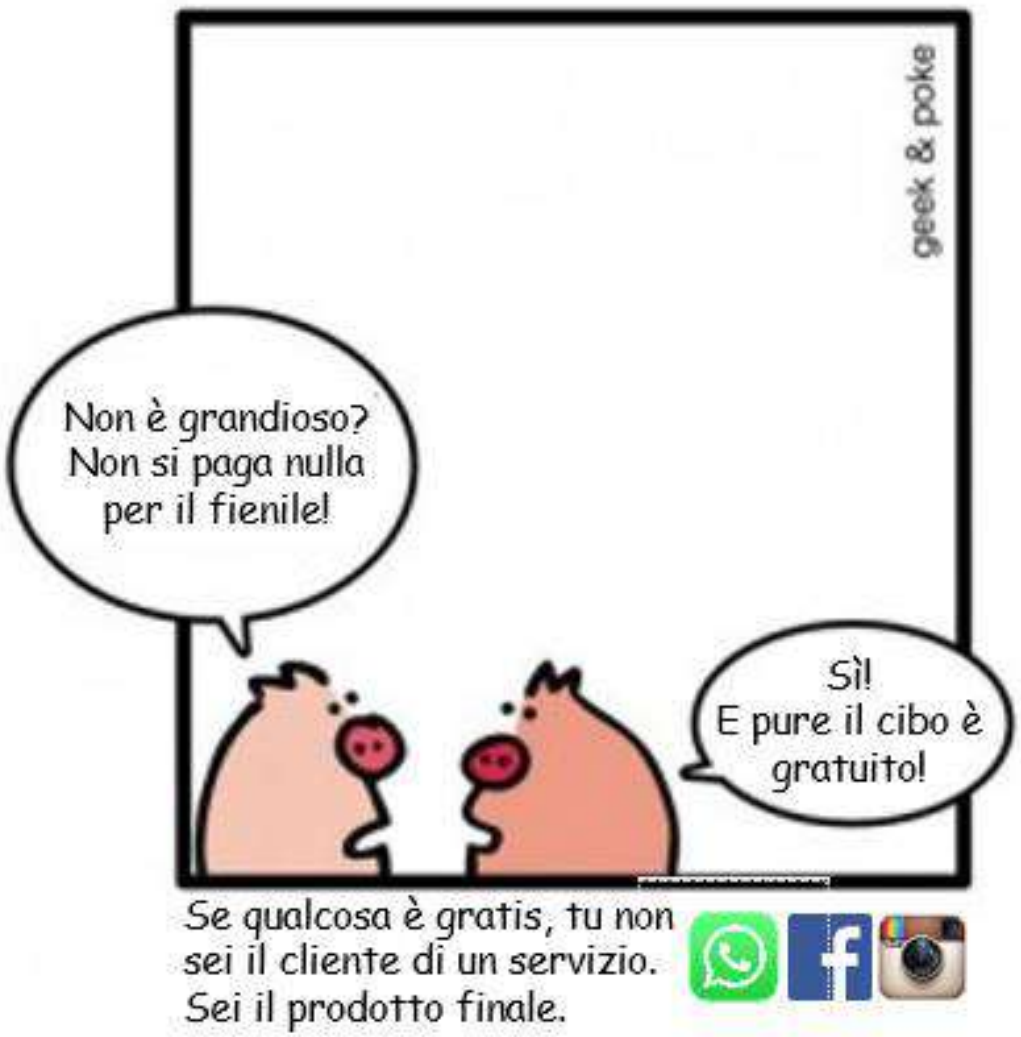
VOLUME
DATA SIZE

VELOCITY
SPEED OF CHANGE

VARIETY
DIFFERENT FORMS OF DATA SOURCES

VERACITY
UNCERTAINTY OF DATA

Il valore delle informazioni



*"Dal 25 maggio sono aumentate di **oltre il 500%** le comunicazioni di data breach al Garante, che hanno interessato, assieme a quelli notificati a partire da marzo, **oltre 330.000 persone.***

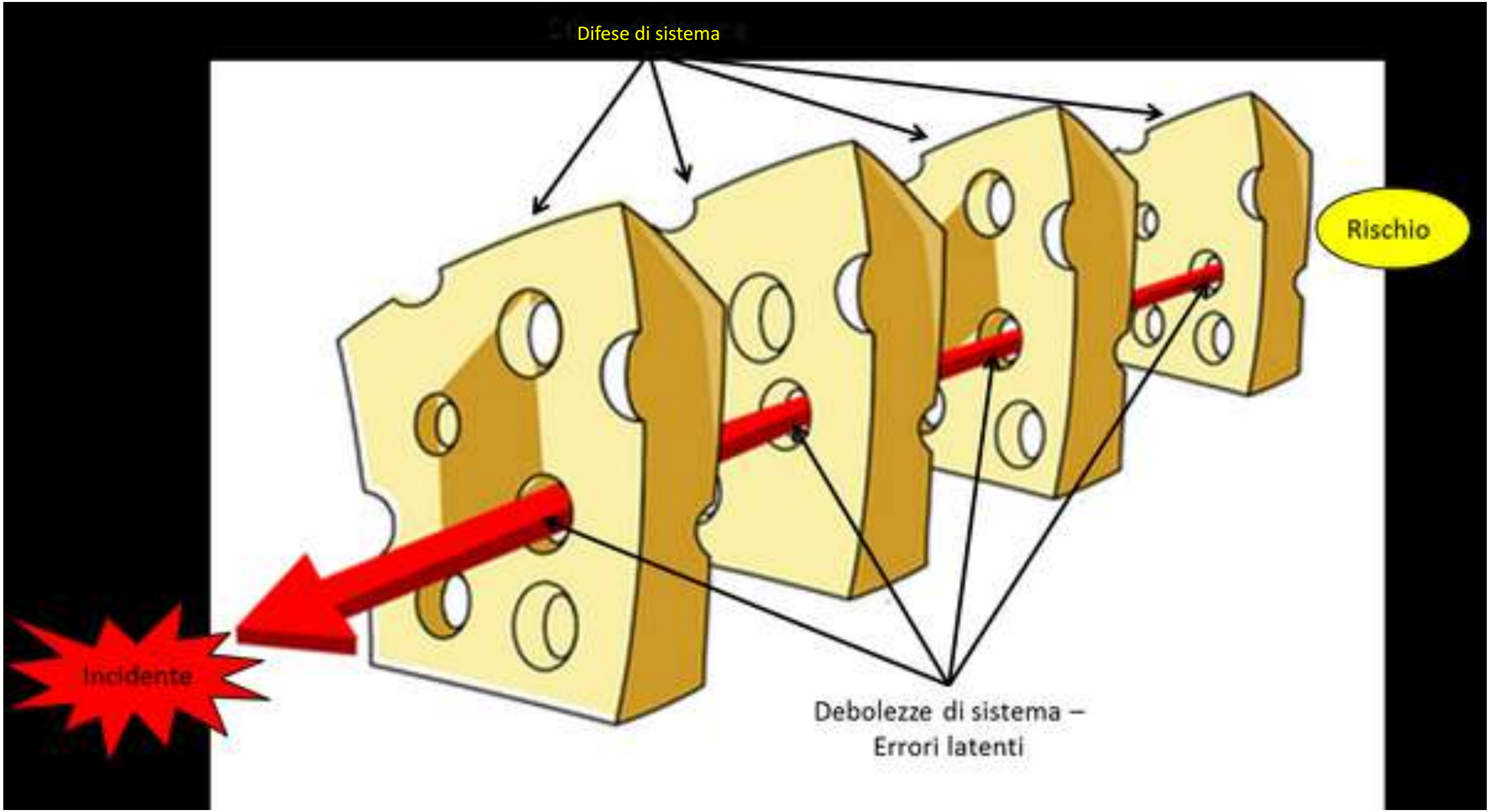
*D'altra parte, in un mondo dove tutto di noi sarà sempre più connesso, **saremo sempre più vulnerabili**, perché ogni oggetto con cui veniamo a contatto può diventare il canale di accesso per un attacco informatico, per una violazione della nostra persona.*

Per questo è indispensabile fare della protezione dei dati una priorità delle politiche pubbliche"

Discorso del Presidente Soro, Roma 10 luglio 2018, p. 5

Impara tutto ciò che ti è possibile dagli errori degli altri. Non avrai tempo a sufficienza per farli tutti.

Non c'è frase più calzante di questa di **Alfred Sheinwold** per capire appieno le caratteristiche, le problematiche e i rischi del mondo digitale e, quindi, le ragioni della protezione dei dati personali.


Difese di sistema
Rischio
Incidente
Debolezze di sistema –
Errori latenti

PREMESSE NORMATIVE

Che cos’è il GDPR?

- Il GDPR non e' solo (e nemmeno "soprattutto") un apparato normativo.

- *è prima di tutto una METODOLOGIA*

- L'errore piu grande che si può fare é considerarlo solo come fonte
- di adempimenti "burocratici".

- E' molto, molto di più. Ma proprio molto di più…

Prof. Francesco Pizzetti

Comunicazione della Commissione al Parlamento europeo e al Consiglio - Bruxelles, 24.1.2018 COM(2018)

«Il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento».

Legge 21 febbraio 1989, n. 98

(ratifica Convenzione di Strasburgo n. 108/1981)

Art. 5 Qualità dei dati

I dati a carattere personale oggetto di un'elaborazione automatizzata sono:

a) ottenuti e elaborati in modo lecito e corretto;

b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini;

c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati;

d) esatti e, se necessario, aggiornati;

e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

Art. 6 Categorie speciali di dati

I dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali.

Art. 7 Sicurezza dei dati

Adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate.

Quali sono le più importanti novità?

- **Principio di trasparenza** (art. 5.1.a GDPR);
- **Principio di responsabilizzazione (accountability)** (art. 5.2);
- **Privacy by design e privacy by default**;
- Rafforzamento diritti degli interessati;
- Analisi dei rischi;
- Verifica dell'efficacia delle misure di sicurezza organizzative e tecniche;
- Adozione di policy aziendali in materia di protezione dei dati personali;
- Qualche novità per gli enti pubblici
- Sanzioni elevatissime
- Superamento del «consensocentrismo»

Ci occupiamo di dati…personali!

REGOLAMENTO (UE) 2018/1807 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 novembre 2018

relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ([1]),

previa consultazione del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

Definizione di dato personale (art. 4.1)

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, i dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Per un approfondimento sul concetto di dato personale si veda il parere n. 4/2007 del Gruppo di lavoro ex art. 29.

Altre definizioni di dati personali

art. 4.13 - dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

art. 4.14 - 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;

art. 4.15 - dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Categorie particolari di dati personali – definizione ricavabile indirettamente dall’art. 9 del GDPR.

Definizione di trattamento (art. 4.2)

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Definizione dell’attività di profilazione (art. 4.4)

Qualsiasi forma di trattamento automatizzato di dati personali effettuato 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

Definizione di pseudonimizzazione (art. 4. 5)

il trattamento dei dati personali in modo tale che gli stessi 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;

per un approfondimento sulle tecniche di anonimizzazione si veda il parere del Gruppo di lavoro art. 29 n. 5/2014 (WP216)

Definizione di consenso (art. 4.11)

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;

Considerando 4

Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

diritto di difesa
diritto di cronaca
diritto dell'impresa
attività di ricerca
diritto alla trasparenza delle PP.AA
legittimo interesse

Principi applicabili al trattamento di dati personali (art. 5)

Paragrafo 1 - I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (idoneità dell'informativa per contenuto e modalità con cui viene resa - cfr. artt. 12, 13 e 14);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (le finalità di archiviazione nel pubblico interesse e quelle di ricerca scientifica o storica non sono considerate incompatibili con quelle iniziali - cfr. art 89)
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 (i dati inesatti devono essere rettificati o cancellati);

Principi applicabili al trattamento di dati personali (art. 5)

e) conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono essere conservati per tempi più lunghi);

f) trattati in modo da garantire un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Paragrafo 2 – Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (principio di responsabilizzazione o accountability)

Liceità del trattamento (art. 6.1)

Il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

Liceità del trattamento (art. 6.1)

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (in particolare se l'interessato è un minore).

Non per le PA

Liceità del trattamento (art. 6.2)

Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del regolamento ai trattamenti necessari per adempiere un obbligo legale al quale è soggetto il titolare o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare

Condizioni per il consenso (art. 7)

- il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

- se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre materie, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

- L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato della possibilità di revocarlo.

- Nel valutare se Il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (art.8)

- 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 il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

- Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

L'art. 2-quinquies del D.lgs. 196/03, introdotto dal D.lgs. 101/2018, prevede un'età di 14 anni

Trattamento di categorie particolari di dati personali (art. 9.1)

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

Trattamento di categorie particolari di dati personali (art. 9.2)

Il divieto non si applica nei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

Trattamento di categorie particolari di dati personali (art. 9.2)

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

Trattamento di categorie particolari di dati personali (art. 9.2)

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

Trattamento di categorie particolari di dati personali (art. 9.2)

g) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sulla base del diritto dell'Unione o di uno Stato membro;

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

GLI ADEMPIMENTI PRINCIPALI NEL REGOLAMENTO PRIVACY UE:

- **adempimenti generali:** trasparenza
(*informativa, consenso, diritto di accesso, diritto alla portabilità dei dati, diritto alla limitazione del trattamento, diritto all'oblio, registro trattamenti, analisi dei rischi)*

- **adempimenti speciali:** accountability
(*notifica «data breach», DPIA e consultazione preventiva*)

- **adempimenti organizzativi:** organizzazione (*formalizzazione rapporti tra titolari e contitolari, titolari e responsabili, responsabili e subresponsabili, responsabili interni (designati) e incaricati (autorizzati), incarico DPO, formazione/istruzioni e misure di sicurezza)*

TRASPARENZA

Informative e contratti…

Considerando 58

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, **facilmente accessibili e di facile comprensione** e che sia usato un **linguaggio semplice e chiaro**, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in **formato elettronico**, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i **minori** meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12)

Il regolamento ha rafforzato il contesto complessivo di garanzie e procedure da osservare nello svolgimento del trattamento e nel rapporto con l'interessato, rendendo più precisi e cogenti gli obblighi incombenti sul titolare;

Il titolare deve adottare misure appropriate per:

- fornire all'interessato l'informativa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori (per iscritto o con altri mezzi compresi quelli elettronici. Su richiesta dell'interessato anche oralmente purchè sia comprovata la sua identità);
- agevolare l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22;

La violazione delle disposizioni relative ai diritti degli interessati, contenute negli articoli da 12 a 22, è soggetta a sanzioni amministrative pecuniarie fino a 20 milioni di euro o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (febbraio 2018)

MODALITA' PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

cosa cambia

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità (il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta).
- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive.
- Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Può essere dato oralmente solo se così richiede l'interessato stesso.
- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13.1 e .2)

- Identità del titolare e dell'eventuale suo rappresentante, nonché i loro rispettivi contatti, compreso quello del DPO se nominato;
- finalità del trattamento;
- base giuridica del trattamento (se il trattamento si base sul perseguimento di legittimi interessi del titolare, questi vanno specificati);
- eventuali obblighi di legge o di contratto di conferire i dati e conseguenze in caso di rifiuto a conferirli;

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13.1 e .2)

- ambito di circolazione dei dati per destinatari o categorie di destinatari, specificando , qualora l'ambito sia esterno all'Unione, se vi è decisione di adeguatezza o, in mancanza, richiamando le garanzie previste agli artt. 46, 47 e 49, secondo comma, nonché indicando dove poterle reperire in forma integrale;
- eventuale processo decisionale basato unicamente su trattamento automatizzato, logica utilizzata e conseguenze per l'interessato;
- periodo di conservazione dei dati personali o, quando non è possibile, i criteri utilizzati per determinare tale periodo;
- diritti dell'interessato: accesso, rettifica/integrazione, cancellazione, limitazione, opposizione, portabilità, reclamo a un'Autorità garante, revoca del consenso nei casi di legge

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13.3)

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, deve fornire all'interessato le seguenti ulteriori informazioni:

- indicazione della nuova finalità;
- periodo di conservazione dei dati personali o, quando non è possibile i criteri utilizzati per determinare tale periodo;
- eventuale processo decisionale basato unicamente su trattamento automatizzato, logica utilizzata e conseguenze per l'interessato;
- diritti dell'interessato: accesso, rettifica/integrazione, cancellazione, limitazione, opposizione, portabilità, reclamo a un'Autorità garante, revoca del consenso nei casi di legge;

Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato (art. 14.1)

In questo caso il contenuto dell'informativa è lo stesso di quella fornita ai sensi dell'art. 13, alla quale vanno aggiunte le seguenti indicazioni:

- origine dei dati personali, precisando se gli stessi provengano eventualmente da fonti accessibili al pubblico;
- categorie di dati personali trattati;

Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato (art. 14.4)

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, deve fornire all'interessato le seguenti ulteriori informazioni:

- indicazione della nuova finalità;
- origine dei dati personali, precisando se provengono da fonti accessibili al pubblico;
- interesse legittimo perseguito dal titolare;
- periodo di conservazione dei dati personali o, quando non è possibile i criteri utilizzati per determinare tale periodo;
- eventuale processo decisionale basato unicamente su trattamento automatizzato, logica utilizzata e conseguenze per l'interessato;
- diritti dell'interessato: accesso, rettifica/integrazione, cancellazione, limitazione, opposizione, portabilità, reclamo a un'Autorità garante, revoca del consenso nei casi di legge;

Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato (art. 14.5)

E' possibile non fornire l'informativa quando:

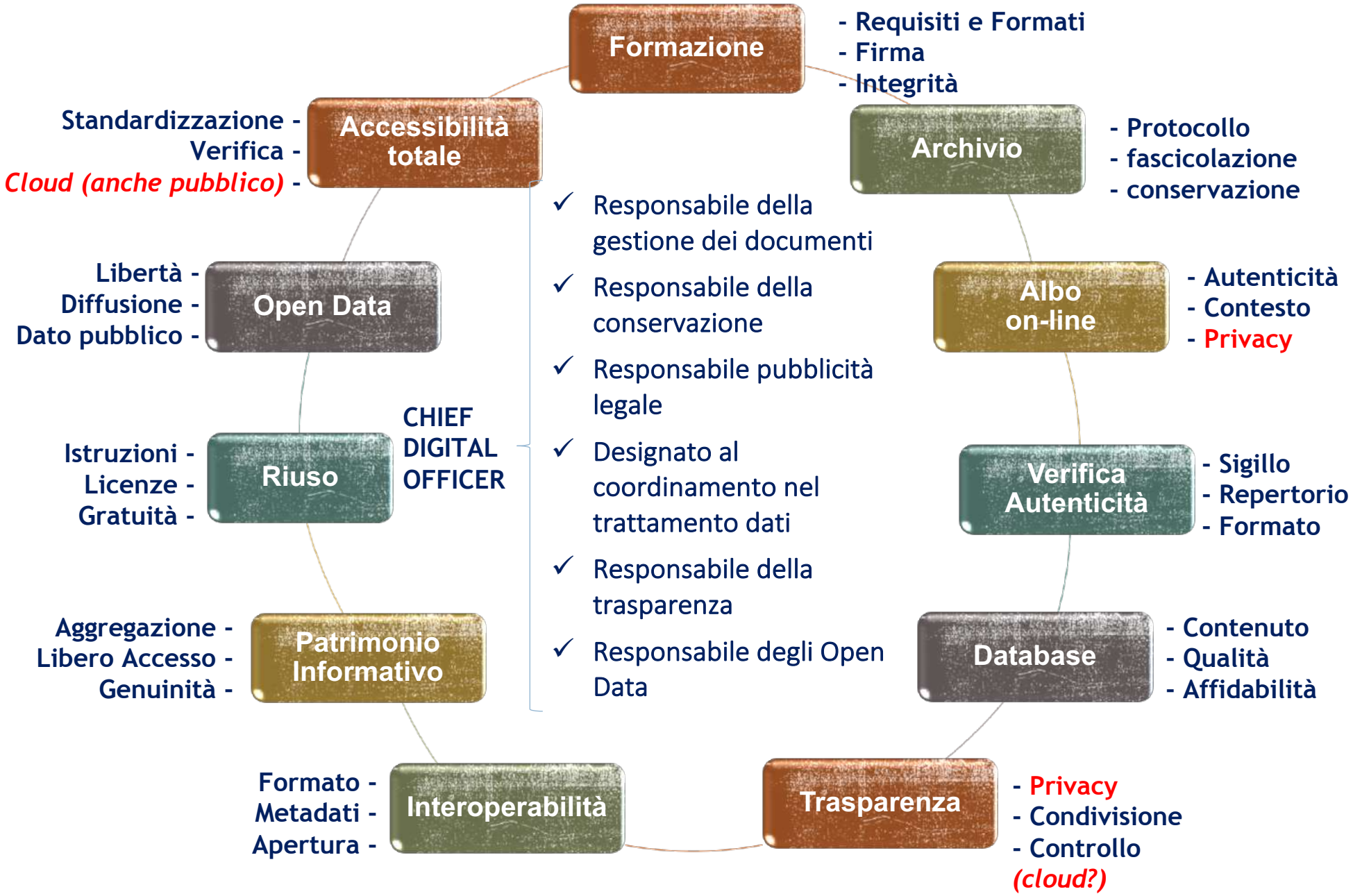
- risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In questi casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Trasparenza necessaria ed effettiva

Effettuare una rigorosa, efficace e trasparente **mappatura di tutti i trattamenti di dati** afferenti alla propria organizzazione, siano essi svolti direttamente dal titolare o affidati all'esterno, costituisce, infatti, il presupposto necessario di ogni azione di assessment:

- ✓Come si può garantire una **efficace informativa** ai sensi degli artt. 13 e 14 del GDPR per gli interessati, se non si conoscono i dettagli dei trattamenti sviluppati in qualità di titolari? Come si possono rendere effettivi i diritti degli interessati se non si ha un controllo trasparente di sistemi informativi, database, sistemi di gestione documentale e archivi?
- ✓Come si può effettuare una esauriente **analisi dei rischi** ai sensi dell'art. 32 del GDPR e implementare adeguate misure di sicurezza se non si è proceduto a verificare attentamente la tipologia di dati trattati e le relative modalità di trattamento?
- ✓Come si può **verificare un software** o svilupparlo disegnandolo secondo i parametri di protezione delineati dal GDPR se non si conoscono nel dettaglio la natura e le finalità del trattamento dei dati e il loro ambito di circolazione?
- ✓Come si possono verificare le **tempistiche di conservazione** dei vari trattamenti dei dati personali se non li si è mappati e verificati con accuratezza?
- ✓Etc.

Il GDPR NELLE VARIE FASI DEL DOCUMENTO INFORMATICO AMMINISTRATIVO



ACCOUNTABILITY

«da un grande potere derivano grandi responsabilità»

Il significato del termine “accountability”

Con il termine “accountability” - che nel mondo anglosassone è di uso comune e il suo significato è ampiamente compreso e condiviso - si deve intendere, in linea generale, l’obbligo:

- di introdurre logiche e meccanismi di responsabilizzazione interna alle aziende e pa relativamente all’impiego delle risorse e alla produzione dei correlati risultati;

- di dar conto all’esterno e in particolare al complesso degli stakeholder, in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati.

Accountability

Il titolare del trattamento deve essere, quindi, in grado di dimostrare di aver adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, (analoghi a quelli utilizzati nell'applicazione del d. lgs. 231/2001).

Aziende e PA devono sviluppare e dotarsi di strumenti che possano essere utilizzati per valutare lo stato della propria accountability e dimostrarlo all'Autorità Garante.

Vd. Parere Gruppo di Lavoro Garanti Europei ex art. 29 – Parere n. 3/2010 adottato il 13 luglio 2010

(l'accountability nasce prima del GDPR come criterio interpretativo della precedente disciplina contenuta nella direttiva 95/46/CE)

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

- Il quadro normativo dell'Unione europea necessita di strumenti aggiuntivi finalizzati a contribuire il passaggio "dalla teoria alla pratica".
- In particolare è necessario introdurre un principio di responsabilità che richieda ai titolari e ai responsabili del trattamento di mettere in atto misure adeguate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati e per dimostrare tale osservanza, su richiesta, alle autorità di controllo.
- L'introduzione del principio di responsabilità deve garantire la certezza del diritto, lasciando spazio al tempo stesso ad una certa adattabilità che consenta di determinare le misure concrete da applicare in funzione dei rischi connessi al trattamento e dei tipi di dati trattati.

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

Le ragioni della necessità di introdurre il principio di responsabilità:

- continuo aumento della quantità di dati personali raccolti, elaborati e condivisi - favorito sia dai progressi tecnologici, sia dalla crescente capacità degli utenti di impiegare le tecnologie e interagire con esse - e conseguente aumento dei rischi di abuso;

- aumento del valore dei dati personali in termini sociali ed economici;

- necessità per i titolari del trattamento di ridurre al minimo i rischi **giuridici**, **economici** e **di reputazione** che possono derivare da una inadeguata protezione dei dati personali.

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

- l'introduzione del principio di responsabilità non comporta nuovi obblighi giuridici in capo ai titolari del trattamento ma è finalizzato a garantire l'effettiva osservanza di quelli esistenti;

- Il principio di responsabilità evita volutamente di precisare nei dettagli il tipo di misure tecniche ed organizzative da attuare, in quanto l'idoneità delle stesse dovrà essere decisa dal titolare del trattamento, caso per caso, tenuto conto in particolare della natura dei dati, delle modalità di trattamento e del rischio specifico;

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

Il WP29 ha proposto, comunque, il seguente elenco non esaustivo di "misure comuni" che soddisfano il principio di responsabilità:

- mappare i processi e gestire il loro inventario (registro attività di trattamento)
- definire procedure interne prima di porre in essere nuovi trattamenti (distribuzione ruoli, pianificazione attività di controllo, privacy by design e privacy by default);
- introdurre policy vincolanti da applicare ai nuovi trattamenti e pubblicarle (es. regolamenti interni, codici di condotta)
- designare un DPO o funzioni similari;
- attuare programmi di formazione, istruzione e sensibilizzazione del personale;

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

- definire procedure per la gestione dei diritti degli interessati;
- istituire un meccanismo interno di gestione dei reclami;
- definire procedure interne per la notifica e la comunicazione delle violazioni della sicurezza (data breach);
- effettuare la valutazione d'impatto sulla protezione dei dati per trattamenti che comportano rischi specifici (DPIA);
- effettuare procedure di verifica per assicurare che tutte le misure siano applicate ed efficaci (audit interni o esterni);

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

- anche la valutazione dell'efficacia delle misure, va effettuata tenendo conto della natura e della quantità dei dati trattati, nonché delle modalità con cui gli stessi vengono trattati e dei particolari rischi che il trattamento comporta.
- l'introduzione del principio di responsabilità sostituisce o riduce gli obblighi amministrativi a carico dei titolari del trattamento quali ad esempio le notificazioni preliminari (cfr. artt. 17 e 37 D.Lgs. 196/03)
- poiché il principio di responsabilità pone l'accento sui risultati da raggiungere, il ruolo delle autorità di controllo si traduce prevalentemente in attività "ex post" piuttosto che "ex ante";

WP29 - Parere 3/2010 sul principio di responsabilità (accountability)

- il principio di responsabilità potrebbe contribuire allo sviluppo di competenze giuridiche e tecniche nel campo della protezione dei dati personali sia internamente alle organizzazioni dei titolari, sia nella forma di servizi esterni;
- l'introduzione del principio di responsabilità può favorire, inoltre, lo sviluppo di meccanismi di certificazione che oltre a contribuire a dimostrare che un titolare del trattamento ha rispettato la normativa, consente allo stesso di acquisire un vantaggio competitivo all'interno del mercato.

Considerando 74

È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, 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. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Il principio di accountability

- Art. 5, paragrafo 2 – Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (principio di responsabilizzazione o accountability)

- Art. 24, paragrafo 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;

Il principio di accountability

- Il Regolamento UE 2016/679 rovescia la prospettiva della disciplina in materia di protezione dei dati personali in quanto tutto il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del titolare del trattamento (accountability);

- Il titolare, quale soggetto che determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza, ha maggiore discrezionalità nel decidere come conformarsi alle disposizioni del nuovo regolamento, ma ha l'onere di dimostrare le ragioni a supporto di tali decisioni e le motivazioni per cui ritiene che le medesime siano compliance con il regolamento.

Il principio di accountability

Chi vi è tenuto?

- tutti, non solo il titolare del trattamento. Anche i responsabili, il DPO e il personale incaricato: cfr. artt. 28.1 (“*garanzie sufficienti*”); 37.5 (“*conoscenza specialistica della materia e delle prassi*”); 39.1.b) (“*formazione e sensibilizzazione del personale*”)

- Il considerando 74 e gli artt. 24.1 e 5.2 non riassumono il principio di accountability

L’accountability va cercata in tutta la struttura del GDPR

Il principio di accountability

Un elemento fondamentale dell'accountability è la revisione dei processi

- Art. 24.1: il titolare deve riesaminare e aggiornare le misure adottate

- Art. 32.1.b): titolare e responsabile devono assicurare su base permanente (quindi continua) riservatezza, integrità, disponibilità, resilienza sistemi ICT

- Art. 35.11: il titolare deve riesaminare il DPIA almeno quando insorgono variazioni del rischio

Il principio di accountability

Il rischio per i diritti e le libertà dell'interessato è la vera chiave di volta (cfr. considerando 75 e 85)

- perdita del controllo dei dati personali;
- limitazione di diritti;
- discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie;
- decifratura non autorizzata pseudonimizzazione;
- pregiudizio alla reputazione;
- compromissione del segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica;

Rischio per i diritti e le libertà

- tenuta dei registri del trattamento (30.5);
- adozione misure di sicurezza (32.1);
- notificazione del *data breach* (33.1, previa valutazione di probabilità)

Elevato rischio per i diritti e le libertà

- valutazione d'impatto (35.1);
- consultazione preventiva (36.1);
- designazione DPO (37.1.b 37.1.c);
- comunicazione *data breach* (previa valutazione di probabilità, 34.1)

Accountability (responsabilizzazione)

- mappatura dati e flussi, censimento finalità (e base giuridica);
- censimento e valutazione rischi;
- misure di compliance del titolare e loro revisione (24.1);
- misure di sicurezza (32.1) in particolare policy, formazione, audit terzi;
- notificazione entro 72h del *data breach* (33.1), comunicazione *data breach* agli interessati senza ingiustificato ritardo (34.1);
- adozione di una procedura per il *data breach*;
- ripetizione ciclica DPIA (35.11);
- designazione di un responsabile che presenti garanzie sufficienti (28.1);
- designazione di un DPO con conoscenza specialistica ed esperienza (30.5);
- sostegno alla formazione continua del DPO (38.2);
- DPO, art. 39.1 lett. a)-c);
- cooperazione con Autorità di controllo

Accountability (rendicontazione)

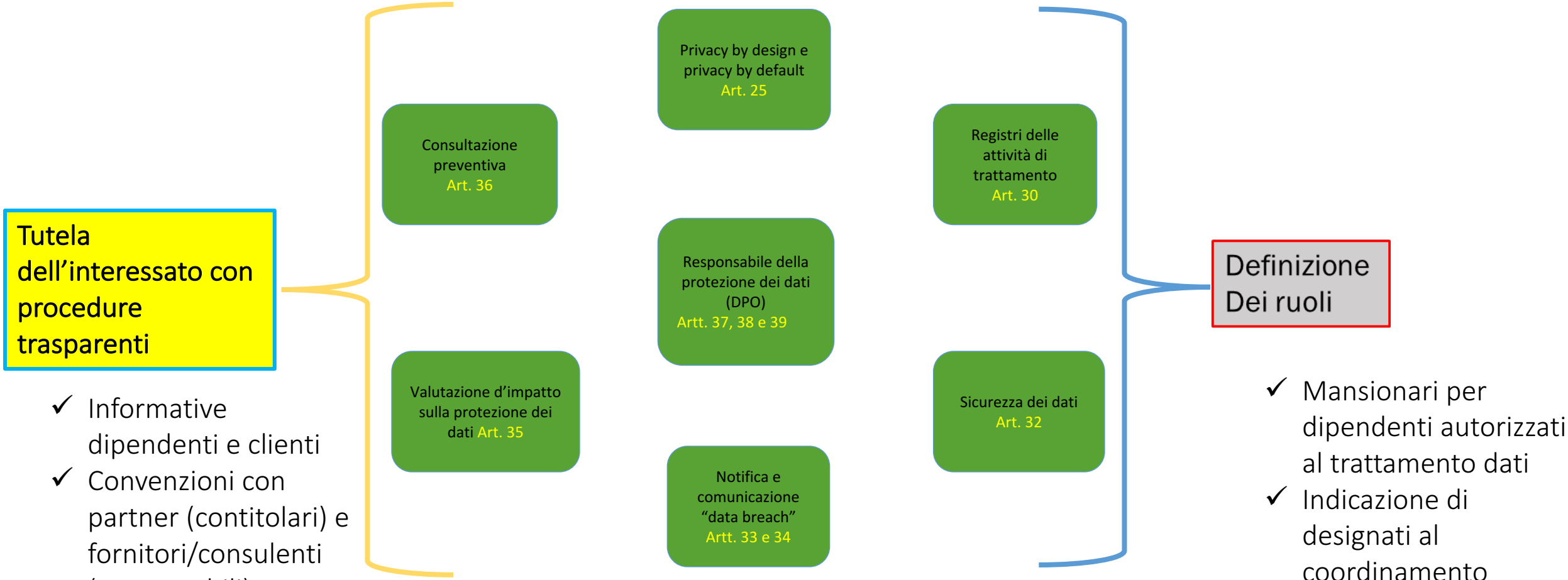
- dimostrazione adozione misure compliance (24.1);
- tenuta dei registri (30);
- dimostrazione adozione misure di sicurezza (32.3);
- tenuta di documentazione *data breach* (33.5);
- documentazione parere DPO su DPIA

Accountability e ruoli nel trattamento (art. 24)

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.

Le principali obbligazioni di compliance previste nel Regolamento UE 2016/679



- ✓ Informative dipendenti e clienti
- ✓ Convenzioni con partner (contitolari) e fornitori/consulenti (responsabili)
- ✓ Garanzie di riscontro

- ✓ Mansionari per dipendenti autorizzati al trattamento dati
- ✓ Indicazione di designati al coordinamento
- ✓ Nomina DPO

PRIVACY BY DESIGN E BY DEFAULT

Considerando 78

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

Considerando 78 (continuazione)

……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.

Protezione dei dati fin dalla progettazione (art. 25.1)

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.

Privacy by design

Protezione dei dati per impostazione predefinita (art. 25.2)

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (by default), 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;
- 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 (es. trattamenti automatizzati)

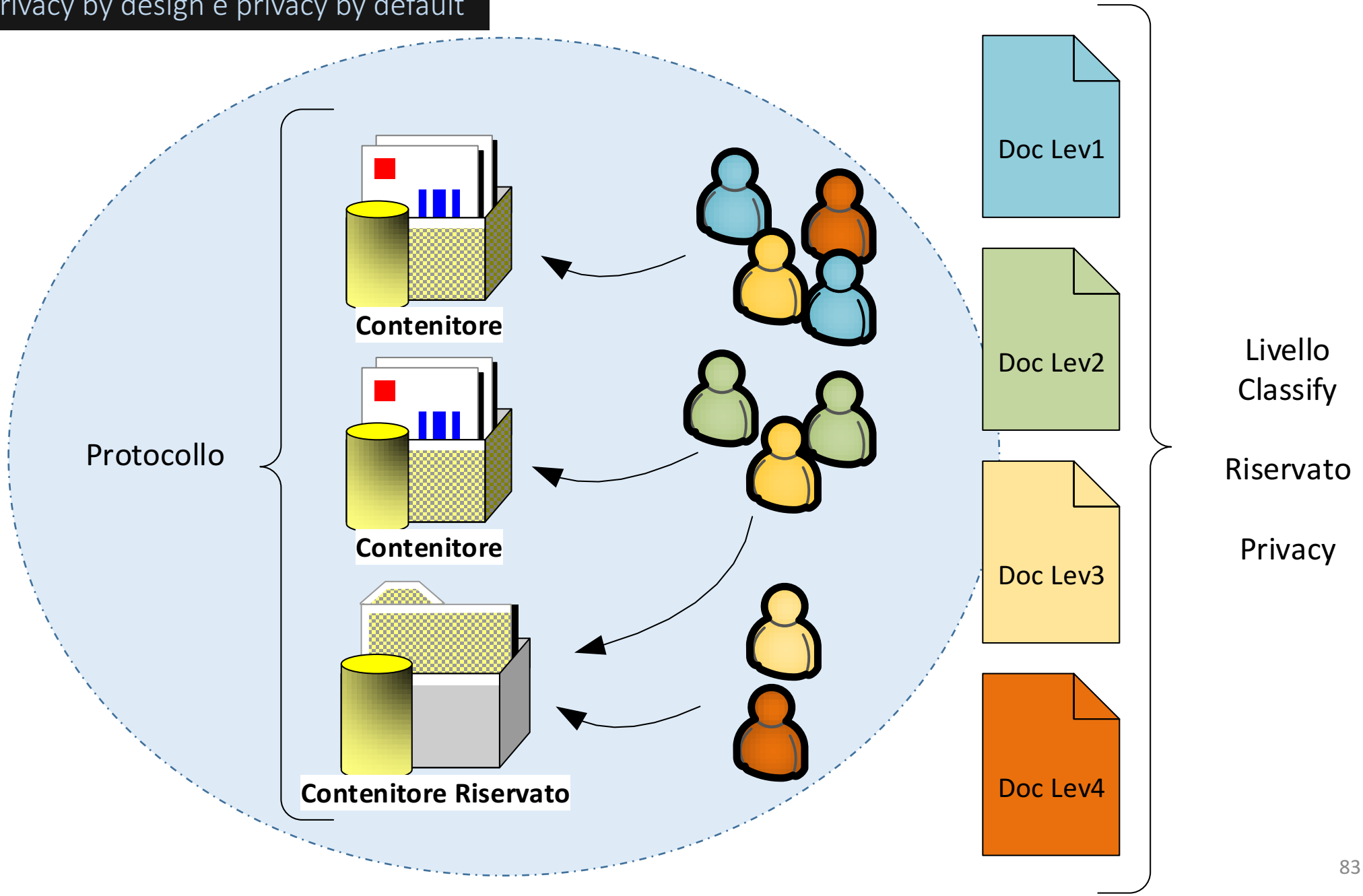
Privacy by default

I 7 principi della Privacy by design

1. Proattivo non reattivo – prevenire non correggere;
2. Privacy come impostazione di default;
3. Privacy incorporata nella progettazione;
4. Massima funzionalità;
5. Sicurezza fino alla fine – piena protezione del ciclo vitale;
6. Visibilità e trasparenza – mantenere la trasparenza;
7. Rispetto della privacy dell'utente – centralità dell'utente.

Approccio metodologico che garantisce una neutra e solida funzionalità operativa indipendentemente da specifiche soluzioni tecnologiche

Esempio di privacy by design e privacy by default



Alcune domande da porre agli applicativi

- ✓ Che attività di trattamento sono consentite dal sw?
- ✓ È consentita la separazione dei dati?
- ✓ È consentita l'esportabilità in formato interoperabile/riutilizzabile dei dati?
- ✓ È consentita la «limitazione» nel trattamento del dato in caso di richiesta?;
- ✓ È prevista l'automatica cancellazione dei dati dopo un tempo stabilito?
- ✓ Ci sono strumenti di anonimizzazione/pseudoanonimizzazione?
- ✓ In caso di soluzione in cloud i server sono dislocati in Europa?
- ✓ È previsto un accesso selettivo ai dati previo inserimento di id e pw?
- ✓ Le pw sono robuste? Il sistema ne prevede in automatico il cambio?
- ✓ Sono previste politiche di autorizzazione differenziata per profilo utente nella gestione dei database?
- ✓ È prevista una gestione dei log?
- ✓ È previsto una gestione dei report in caso di data breach?
- ✓ Etc.

Ovvio che tutto va analizzato sempre in base ai dati trattati, al concetto di larga scala, alle modalità del trattamento etc.

Il percorso di adeguamento al GDPR

FASE - 1
Valutazione della compliance (audit)

FASE - 2
Impostazione del registro dei trattamenti

FASE - 3
Individuazione dei ruoli e delle responsabilità

FASE - 4
Stesura e/o modifica della documentazione

FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza

FASE - 6
Implementazione del processo di data breach

FASE - 7
Definizione delle modalità per la valutazione di impatto

FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase I - Una, nessuna, centomila check list

Una **“check list”** con domande specifiche da fare è il primo passo per entrare in contatto con la nostra realtà professionale, aziendale e/o amministrativa.

Il primo identikit da tracciare è quello del reparto già impegnato ad occuparsi direttamente della materia (in genere quello amministrativo o informatico, o legale…sperando che questo reparto realmente esista!) allargando il tratto ad altri uffici più “delicati”, sulla base dei trattamenti di dati posti in essere al loro interno (ad esempio il reparto risorse umane, o l’ufficio marketing e comunicazione, quello IT e così via).

Le check list consentono di effettuare un primo screening delle criticità e degli eventuali gap da colmare e, quindi, di avviare la successiva pianificazione degli interventi necessari. In questa fase, si può già riconoscere se la realtà con cui si ha a che fare debba dotarsi obbligatoriamente di un DPO (Data Protection Officer) o se per natura e dimensioni è in grado di auto regolamentarsi.

Fase 1 – Processo di assessment

- Mappare gli strumenti e le risorse informatiche interne:
  - gestionali utilizzati
  - tipologia sistemi operativi utilizzati
  - gestione posta elettronica e PEC

- Mappare eventuali trattamenti elettronici particolari quali ad esempio:
  - presenza di sistema di videosorveglianza
  - utilizzo di strumenti biometrici
  - utilizzo di strumenti GPS
  - utilizzo di strumenti RFID
  - presenza di dispositivi o risorse informatiche a utilizzo promiscuo

- Mappare le banche dati (dipendenti, clienti, fornitori, fatturazione elettronica, newsletter)

Fase 1 – Processo di assessment

- Mappare gli strumenti e le risorse fisiche interne quali ad esempio:
  - presenza di un sistema d'allarme
  - presenza di aree o di contenitori ad accesso selezionato e gestione delle chiavi
  - presenza di strumenti distruggi documenti
  - gestione di dorsi di raccoglitori, intestazione di fascicoli, ecc.

- Mappare gli strumenti e le risorse organizzative interne quali ad esempio:
  - presenza di policy per la gestione dei *data breach*
  - presenza di policy per il riscontro agli interessati
  - presenza di policy per l'utilizzo della posta elettronica e Internet
  - presenza di policy in materia di sicurezza fisica e buone prassi
  - presenza di policy per l'utilizzo in modalità BYOD

Fase 1 – Processo di assessment 32

- Individuazione dei soggetti esterni e dei relativi flussi di dati coinvolti, es.:
  - accesso dall'esterno a risorse aziendali (es. via VPN)
  - fornitori di servizi di manutenzione e vigilanza
  - fornitori di servizi di assessment e certificazione
  - fornitori servizi informatici
  - fornitori di servizi contabili/tributari/elaborazione buste paga
  - fornitori di servizi legali
  - fornitori di servizi in materia di medicina del lavoro
  - banche e servizi di pagamento
  - soggetti pubblici
  - sindacati

destinatari esterni di trattamento, per tipologie diverse di trattamenti (attenzione ai flussi esterni oltre i confini della UE/SEE)

FASE - 1
Valutazione della compliance (audit)

FASE - 2
Impostazione del registro dei trattamenti

FASE - 3
Individuazione dei ruoli e delle responsabilità

FASE - 4
Stesura e/o modifica della documentazione

FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza

FASE - 6
Implementazione del processo di data breach

FASE - 7
Definizione delle modalità per la valutazione di impatto

FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

FASE 2 - Impostazione del registro dei trattamenti

Con le informazioni raccolte durante le attività di assessment, cominciare ad implementare il registro delle attività di trattamento, riportando nello stesso:

- Le diverse tipologie di dati personali trattati (anagrafici, sanitari, «sensibili», biometrici, genetici, giudiziari);
- le categorie di interessati (dipendenti, clienti, fornitori, utenti sito web, ecc.);
- la finalità del trattamento e la base giuridica che lo legittima (artt. 6 e 9) → particolare attenzione deve essere prestata al legittimo interesse (cfr. provvedimento del Garante del 22.02.2018 – doc. web n. 8080493);
- le modalità con cui vengono trattati i dati (manuale, parzialmente o interamente automatizzato);

FASE 2 - Impostazione del registro dei trattamenti

- Le categorie dei destinatari sia interni (es. uffici) che esterni (autonomi titolari, contitolari e responsabili ex art. 28 del GDPR);
- gli eventuali trasferimenti di dati personali verso paesi extra UE o organizzazioni internazionali (è necessario indicare il paese e le garanzie adottate previste negli artt. da 44 a 49 del GDPR);
- I tempi di cancellazione dei dati per ogni trattamento;
- Le misure organizzative e tecniche adottate;
- Le modalità con cui viene raccolto il consenso nei casi in cui questo rappresenta la base giuridica che legittima il trattamento;

Fase 2 - Impostazione del registro dei trattamenti

L’introduzione di un registro obbligatorio delle attività svolte è prevista espressamente dall’art. **30 del GDPR** ed è stata più volte ribadita e caldeggiata del Garante. Obbligatorietà che si fa duplice, poiché - oltre a riguardare il possesso dello stesso - a essere obbligatoria è soprattutto la sua corretta, aggiornata e puntuale compilazione.

Tale registro, infatti, contiene tutta una serie di indicazioni che permettono da un lato di adeguarsi alla norma, dall’altro di creare delle procedure (sartoriali) rispetto ai sistemi di gestione interni.

Considerando 82

Per dimostrare che si conforma al presente regolamento, il titolare o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

Contenuti del registro tenuto dal titolare del trattamento (art. 30.1)

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del DPO;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e della natura dei dati personali (identificativi, relativi alla salute, biometrici, genetici, giudiziari)
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

Contenuti del registro tenuto dal titolare del trattamento (art. 30.1)

- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (compresa la loro identificazione). Per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Cfr. art. 38, comma 2, del D.lgs. 196/03 (oggi abrogato) – contenuti della notifica al Garante

Contenuti del registro tenuto dal responsabile del trattamento (art. 30.2)

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all’art. 30.1;

Suggerimento: ulteriori opportune informazioni che si potrebbero inserire nel registro

L'obbligo di tenere il registro delle attività di trattamento potrebbe essere l'occasione per raccogliere ulteriori utili informazioni rispetto a quelle indicate nell'art. 30 del GDPR, quali ad esempio;

- attività effettuate
- base giuridica del trattamento
- elenco terzi coinvolti
- analisi del rischio per singolo applicativo e/o servizio
- esistenza di valutazione d'impatto e consultazione preventiva
- documentazione a supporto del trattamento (es. informativa e consenso)
- procedure per l'esercizio dei diritti dell'interessato
- provvedimenti specifici dell'autorità di controllo

Deroga all'obbligo di tenere il registro delle attività di trattamento (art. 30.5)

Il registro delle attività di trattamento non è obbligatorio - né per il titolare né per il responsabile del trattamento - nel caso in cui le rispettive imprese o organizzazioni hanno meno di 250 dipendenti, a meno che il trattamento che esse effettuano:

- possa presentare un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa il trattamento di dati sensibili o giudiziari;

La doppia funzione del registro delle attività di trattamento

Strumento operativo che:

1. consente di:

- censire le banche dati e i trattamenti in essere;
- rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
- costituire lo strumento di pianificazione e controllo delle attività di trattamento dei dati personali in modo da garantire la loro integrità, riservatezza e disponibilità;
- ridurre gli sprechi in termini di tempo, risorse, duplicazione delle informazioni;
- ridurre i rischi di eventuali trattamenti illeciti.

La doppia funzione del registro delle attività di trattamento

2. Conservare in maniera ordinata e verificabile da terzi le informazioni relative all'adozione delle misure tecniche ed organizzative adeguate ed efficaci finalizzate ad attuare il principio di responsabilizzazione

L'art. 30.3 prevede che i registri del titolare e del responsabile del trattamento siano tenuti in forma scritta - anche in formato elettronico - in modo non solo di poter dimostrare la rispondenza dei trattamenti alla normativa vigente, ma anche poter adempiere all'onere della prova nei casi in cui debba essere valutata la responsabilità del titolare e del responsabile;

L'art. 30.4, infatti, stabilisce che, su richiesta dell'autorità di controllo, tale registro debba essere messo a sua disposizione

FAQ del Garante sul Registro delle attività di trattamento

Il Garante precisa nelle sue FAQ che *le imprese e le organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti a un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento)*. E in ogni caso, anche al di fuori dei casi di tenuta obbligatoria del registro, alla luce del considerando 82 del RGPD, **il Garante *ne raccomanda la redazione a tutti i titolari e responsabili del trattamento***, *in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.*

I registri, quindi, non vanno mai considerati come documenti finiti, ma pensati come **schema di riferimento** che può per esigenze dinamiche e temporali essere plasmato senza snaturarsi della propria natura di raccolta e conservazione.

Aggiornamento del registro delle attività di trattamento

- diversamente da quanto prevedeva il Codice privacy per il Documento Programmatico sulla Sicurezza, il GDPR non prevede una data e neppure un obbligo espresso di aggiornamento del registro delle attività di trattamento.

- ma allora.....il registro delle attività di trattamento bisogna aggiornarlo periodicamente? e con quale periodicità?

Principio di accountability: il titolare deve non solo garantire che i trattamenti che effettua sono conformi al GDPR, ma anche essere in grado di dimostrarlo!!!!

Un possibile modello di registro delle attività di trattamento

Identificativo Trattamento	Finalità	Base Giurifica del trattamento		Categorie di dati personali			Tipi di dati personali trattati	Catgeoria di interessati	Categoria di destinatari		Modalità del trattamento dei dati personali	Luogo di custodia dei dati personali	Termini di conservazione	Misure di sicurezza	DPIA	Trasferimento paesi	
		Liceità ex art 6 GDPR	Liceità ex art. 9 GDPR						Interni	Esterni						Paese	Garanzie adottate

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Registro titolare: modello semplificato suggerito dal GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*		
RESPONSABILE *[inserire la denominazione e i dati di contatto]*		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*		
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*		
CATEGORIA DI TRATTAMENTO	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Registro responsabile: modello semplificato suggerito dal GPDP

FASE - 1
Valutazione della compliance (audit)

FASE - 2
Impostazione del registro dei trattamenti

FASE - 3
Individuazione dei ruoli e delle responsabilità

FASE - 4
Stesura e/o modifica della documentazione

FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza

FASE - 6
Implementazione del processo di data breach

FASE - 7
Definizione delle modalità per la valutazione di impatto

FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase III - Definire i principali attori e loro responsabilità

Dopo aver compiuto questi primi importanti passi, ci troviamo in una fase intermedia del nostro processo di assessment, un punto cruciale dell'intera attività. Un momento questo, in cui abbiamo a disposizione una **mappatura completa dei flussi dei dati personali sia all'interno che all'esterno dell'organizzazione** e quindi, da adesso fino alla fine del processo di adeguamento, saranno le scelte del "professionista della privacy" a fare la differenza. Scelte che vertono essenzialmente sulle dinamiche procedurali come:

- **l'individuazione di contitolari e dei responsabili del trattamento** in linea con i principi sanciti dagli articoli 26 e 28 del GDPR e la **definizione dei contenuti vincolanti del contratto o di altro atto giuridico**;
- la **profilazione di eventuali referenti interni** per la gestione delle politiche aziendali in materia di protezione dei dati personali;
- la definizione di un **sistema di controllo periodico** (audit interno) che consenta il costante monitoraggio del livello di compliance con il GDPR;
- la definizione di un **piano formativo** in grado di armonizzare le competenze interne delle diverse funzioni coinvolte.

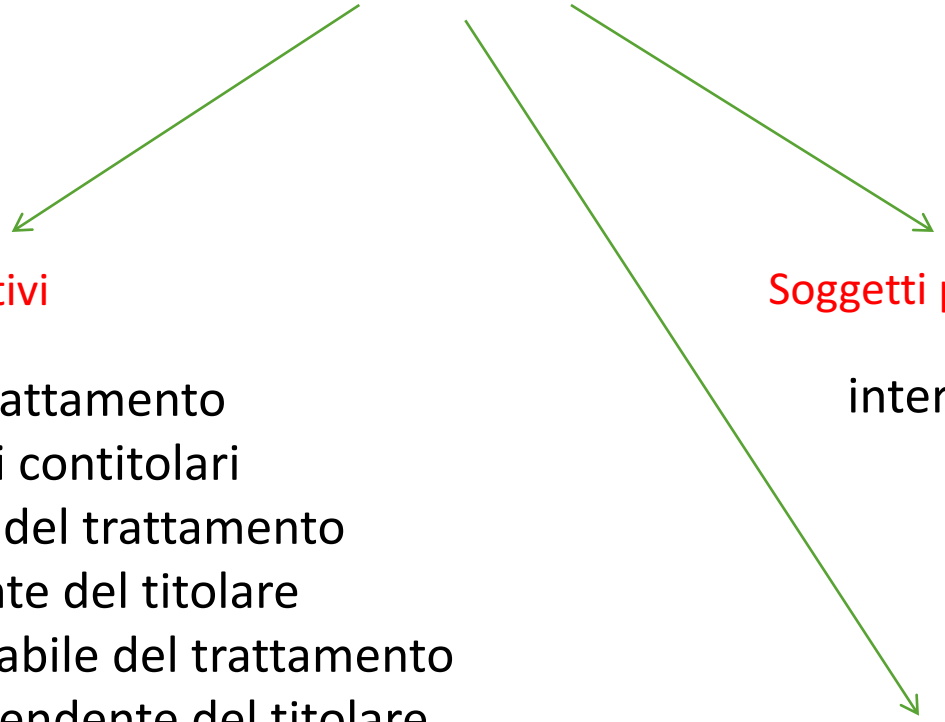
Dopo aver definito l'organigramma privacy, non ci resta che avviarci così a un indispensabile **check generale del lavoro svolto fino ad ora**, così da poter rilevare e correggere eventuali gap (normativi e applicativi) tra quanto svolto (compreso la redazione della documentazione obbligatoria) e lo spirito (funzionale) del GDPR.

I RUOLI e LE RESPONSABILITÀ:

Con il Regolamento UE viene in parte ridisegnato l'organigramma privacy, con l'introduzione di nuove figure soggettive e l'attribuzione di nuovi compiti e responsabilità:

- Titolare del trattamento (*data controller*);
- Contitolare (*joint controller*);
- Responsabile del trattamento (*data processor*);
- Sub-responsabile (*subprocessor*);
- Responsabile della protezione dei dati o *Data Protection Officer* (DPO).

I soggetti del trattamento



Soggetti attivi

- ✓ Titolare del trattamento
  e gli eventuali contitolari
- ✓ Responsabile del trattamento
- ✓ Rappresentante del titolare
  o del responsabile del trattamento
- ✓ Personale dipendente del titolare
  o del designato del trattamento

Soggetti passivi

interessati

Responsabile della protezione
dei dati personali (DPO)

“attribuzioni e compiti ai soggetti designati”

Vengono inoltre confermati nel decreto di adeguamento rilevanti specificazioni in materia di “attribuzioni e compiti ai soggetti designati” che permetteranno di gestire e applicare, anche nella propria organizzazione interna, l’importante principio dell’accountability che pervade la normativa europea.

In particolare viene precisato nel decreto che

“il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

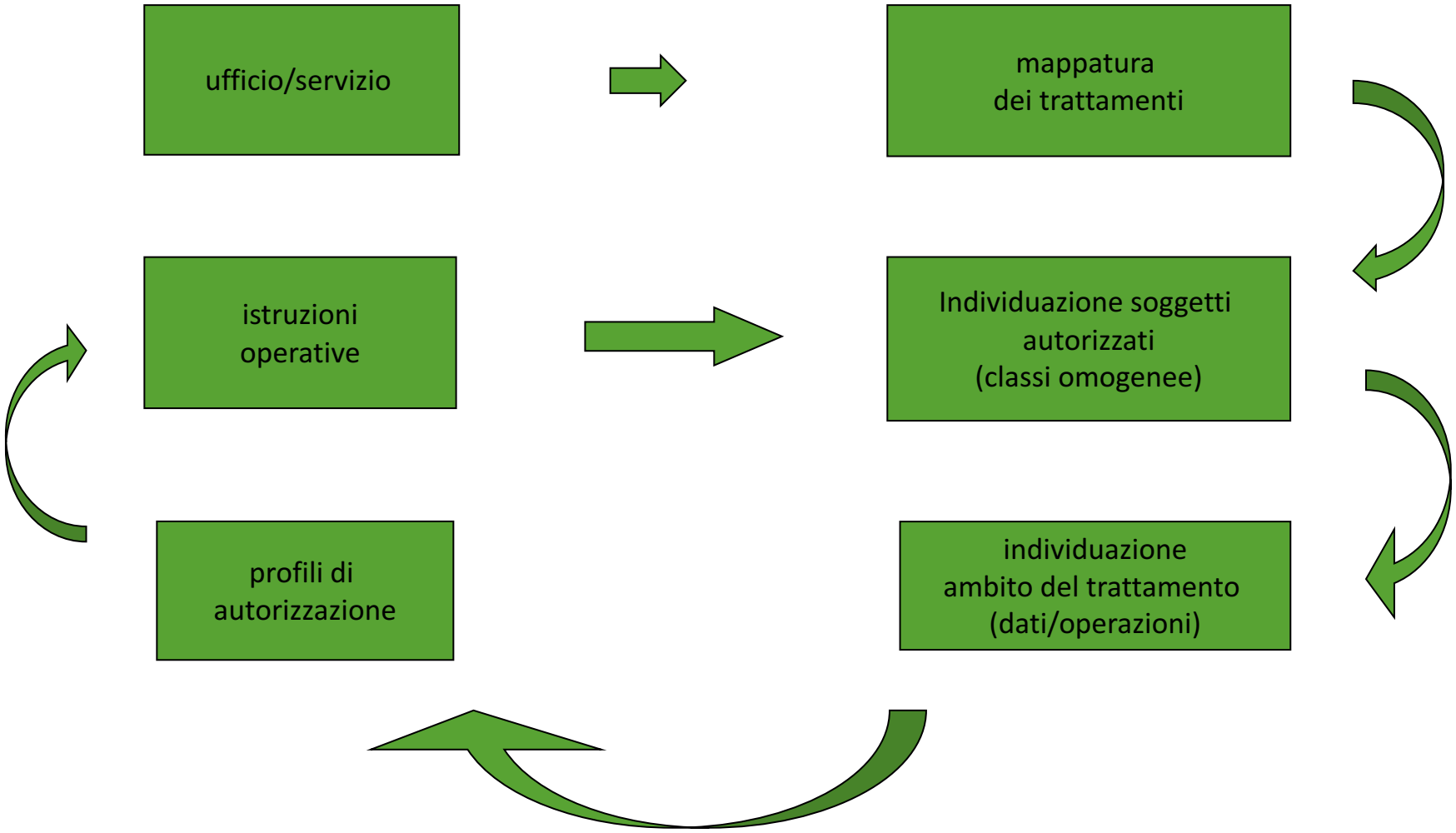
Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta”

(art. 2-quaterdecies del Codice – attribuzione di funzioni e compiti a soggetti designati).

“attribuzioni e compiti ai soggetti designati”

Nella **relazione illustrativa** al decreto, in commento all’art. 2 – terdecies si legge che “la norma prevede il potere di Titolare e Responsabile, di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designati. Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all’organizzazione che, ai sensi del previgente codice in materia di protezione dei dati ma in contrasto con il regolamento, potevano essere definiti, a seconda dei casi, Responsabili o Incaricati.”

Processo per la definizione e gestione dei profili di autorizzazione



Newsletter del GPDP del 7 febbraio 2019 – Consulenti del lavoro: quando sono responsabili del trattamento dei dati?

- I consulenti del lavoro sono titolari quando trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche, come ad esempio i liberi professionisti, determinando puntualmente le finalità e i mezzi del trattamento;

- Sono, viceversa, responsabili quando trattano i dati dei dipendenti dei loro clienti sulla base dell'incarico ricevuto, che contiene anche le istruzioni sui trattamenti da effettuare. E' il caso, ad esempio, dei consulenti che curano per conto di datori di lavoro la predisposizione delle buste paga, le pratiche relative all'assunzione e al fine rapporto, o quelle previdenziali e assistenziali, trattando una pluralità di dati personali, anche sensibili, dei lavoratori.

L'organizzazione aziendale 2.0

In strutture complesse gerarchia
di responsabili/designati a più livelli

CDO

- Titolare autonomo
- Contitolare
- Responsabile esterno

DPO

Solo PA

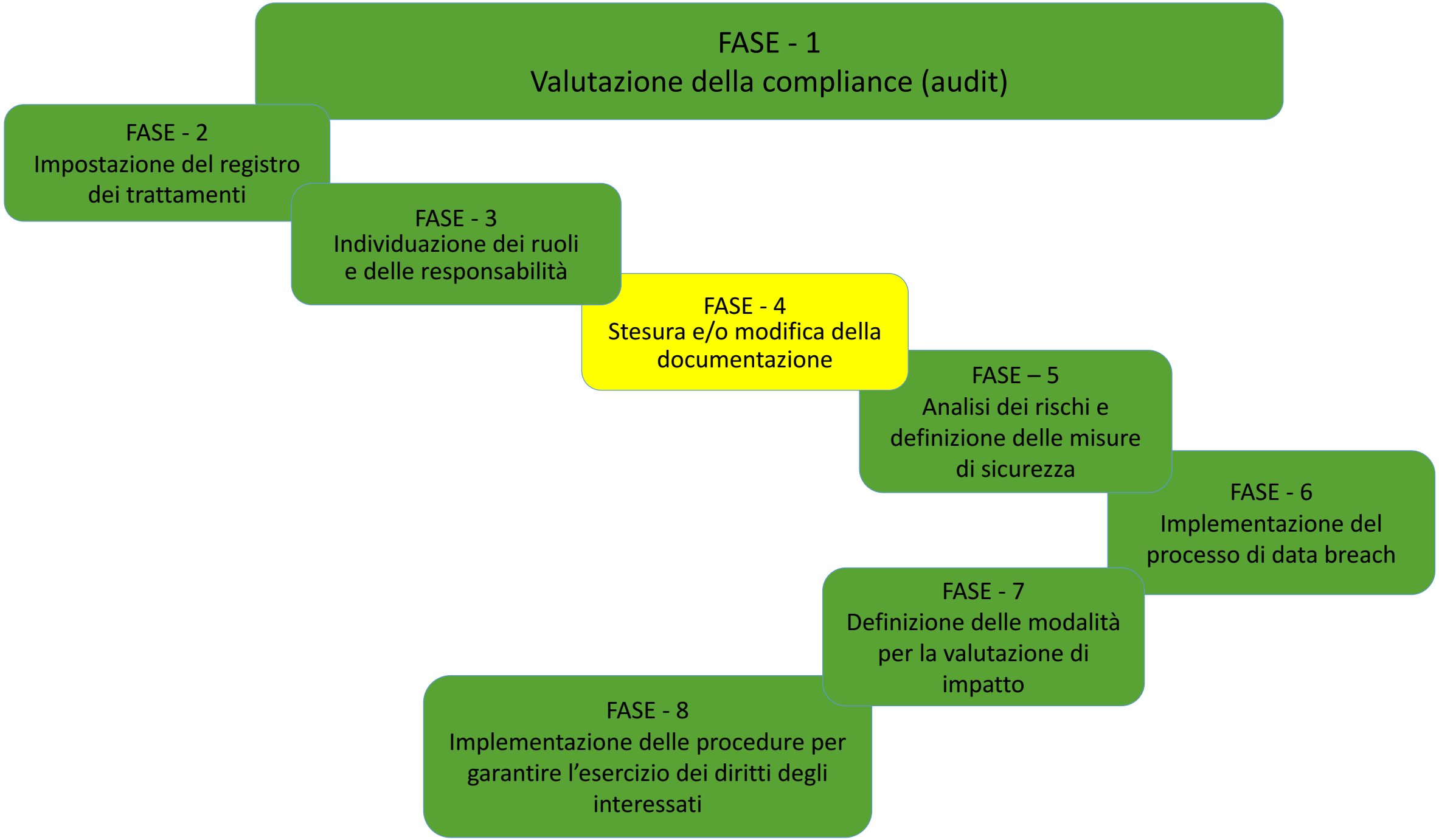
La Governance del patrimonio informativo di una società o una PA:
Compliance normativa nella Società dell'Informazione

Il DPO nel processo di accountability

Il GDPR ha definitivamente chiarito gli **obblighi incombenti sul titolare**, rafforzando il complesso di garanzie e procedure da osservare minuziosamente nel rapporto con gli interessati, attraverso l'implementazione di **procedure finalizzate ad agevolare l'osservanza degli obblighi stabiliti per i responsabili del trattamento dei dati e l'esercizio dei diritti da parte degli interessati**. Si ha spesso una percezione distorta delle procedure, concepite generalmente come qualcosa di rigido e poco funzionale al naturale decorso di vita operativo delle organizzazioni, più o meno complesse. Il GDPR esorta invece a ridisegnare queste procedure, in maniera sartoriale **rispetto alle esigenze della propria organizzazione di riferimento**, sulla base delle reali necessità esistenti, in modo che esse consentano proattivamente di **rispettare i principi previsti dall'art. 5 del GDPR**, verificando anche se – pur in caso di assenza di obbligo – non sia utile dotarsi comunque di un DPO (Data Protection Officer o Responsabile per la protezione dei dati personali). Il DPO, infatti, è un professionista (sia esso soggetto interno o esterno all'organizzazione di riferimento) che deve svolgere una funzione con **competenze multidisciplinari e trasversali tra loro**, rispetto alle materie trattate.

Il DPO nel processo di accountability

La responsabilità principale del DPO è quindi quella di **osservare, valutare e organizzare la gestione del trattamento di dati personali** (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. E proprio in merito alla figura del DPO, credo sia doveroso richiamare la **recente sentenza del TAR Friuli Venezia Giulia n. 287/2018**, che ha con autorevolezza affermato il principio della non obbligatorietà (e oserei dire superfluità) delle **certificazioni** per svolgere questa delicata funzione, sottolineandone la necessaria competenza anche in ambito giuridico. È utile ricordare che al coro di voci negative sulle certificazioni del DPO si è aggiunta anche quella altrettanto autorevole del **Gruppo ex art. 29 direttiva 95/46/CE** (oggi Comitato europeo per la protezione dei dati ex art. 68 del GDPR), che già da tempo ha tenuto a precisare in modo lapalissiano nelle **Linee guida sulle certificazioni** quanto segue: *To further specify what may be certified under the GDPR, the GDPR contains additional guidance. It follows from Article 42.7 that certifications under the GDPR are issued only to data controllers and data processors, which rule out for instance the certification of natural persons, such as data protection officers for example*.


FASE - 1
Valutazione della compliance (audit)
FASE - 2
Impostazione del registro dei trattamenti
FASE - 3
Individuazione dei ruoli e delle responsabilità
FASE - 4
Stesura e/o modifica della documentazione
FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza
FASE - 6
Implementazione del processo di data breach
FASE - 7
Definizione delle modalità per la valutazione di impatto
FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase 4 - Stesura e/o modifica della documentazione

Dopo un attento esame della documentazione raccolta durante la fase 1 è necessario:

- **aggiornare** la documentazione esistente per renderla conforme al GDPR:
  - informative (artt. 13 e 14)
  - moduli di consenso (artt. 7 e 8)
  - eventuali accordi con contitolari (art. 26)
  - eventuali contratti o altri atti giuridici con i responsabili esterni (art. 28)
  - autorizzazioni (art. 29)
  - policy aziendali
- **predisporre** la documentazione mancante;

Informative

Il paradosso informativo:

troppe informazioni disinformano

inoltre

Informazioni disorganizzate disinformano

WP260 “Linee guida sulla trasparenza”

La trasparenza è un obbligo trasversale che deve essere rispettato quando il titolare del trattamento:

- fornisce agli interessati le informazioni relative al trattamento dei dati;
- comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento;
- definisce le modalità con le quali il titolare del trattamento agevola agli interessati l’esercizio dei diritti di cui godono;

WP260 “Linee guida sulla trasparenza”

Le linee guida contengono oltre che un supporto interpretativo sul nuovo obbligo di trasparenza, anche orientamenti pratici riguardanti l’utilizzo di:

- forme concise e trasparenti;
- un linguaggio semplice e chiaro, in particolare quando le informazioni sono rivolte ai minori;
- modalità e strumenti per garantire una facile accessibilità alle informazioni soprattutto in ambiente online.

WP29 - Parere 05/2012 sul cloud computing

Potenziali rischi del cloud computing
per la protezione dei dati

Mancanza di un adeguato controllo da parte del titolare del trattamento sui dati

Mancanza o carenza di informazioni riguardanti Il trattamento dei dati (trasparenza)

Quadro normativo di riferimento per i contratti con i responsabili del trattamento nei servizi di conservazione documentale

- ✓ D.Lgs. 82/2005 “Codice dell’amministrazione digitale”: articolo 44
- ✓ DPCM 3.12.2013 – Regole tecniche in materia di conservazione
- ✓ Circolare AGID n. 65 del 10 aprile 2014 relativa all’accreditamento conservatori
- ✓ Circolari AGID n.2 dedicata alla qualificazione dei servizi CSP e n. 3 relativa ai servizi SaaS, entrambe del 9 aprile 2018.

Art. 44, comma 1-bis, del D.Lgs. 82/2005 (CAD)

Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del D.Lgs 196/03, ove nominato (cfr. art. 2-quaterdecies del novellato D.Lgs. 196/03) e con il responsabile del sistema della conservazione dei documenti informatici, nella definizione e gestione delle attività di rispettiva competenza.

Art. 44, comma 1-ter, del D.Lgs. 82/2005 (CAD)

Il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle linee guida.

Art. 44, comma 1-quater, del D.Lgs. 82/2005 (CAD)

Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali (cfr. art. 2-quaterdecies del novellato D.Lgs. 196/03), con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, tecnologiche e di protezione dei dati personali (contratto o altro atto giuridico ex art. 28 GDPR).

DPCM 3.12.2013 – Regole tecniche in materia di sistema di conservazione

Art. 2 – Ambito di applicazione

comma 3 – le presenti regole tecniche si applicano nel rispetto della disciplina rilevante in materia di tutela dei dati personali

DPCM 3.12.2013 – Regole tecniche in materia di sistema di conservazione

Art. 6 – Ruoli e responsabilità

comma 8 - Il soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali (ora art. 28 del GDPR)

comma 9 - Resta ferma la competenza del Ministero dei beni e delle attività culturali e del turismo in materia di tutela dei sistemi di conservazione degli archivi pubblici e degli archivi privati che rivestono interesse storico particolarmente importante

DPCM 3.12.2013 – Regole tecniche in materia di sistema di conservazione

Art. 10 – Modalità di esibizione

Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva secondo le modalità descritte nel manuale di conservazione

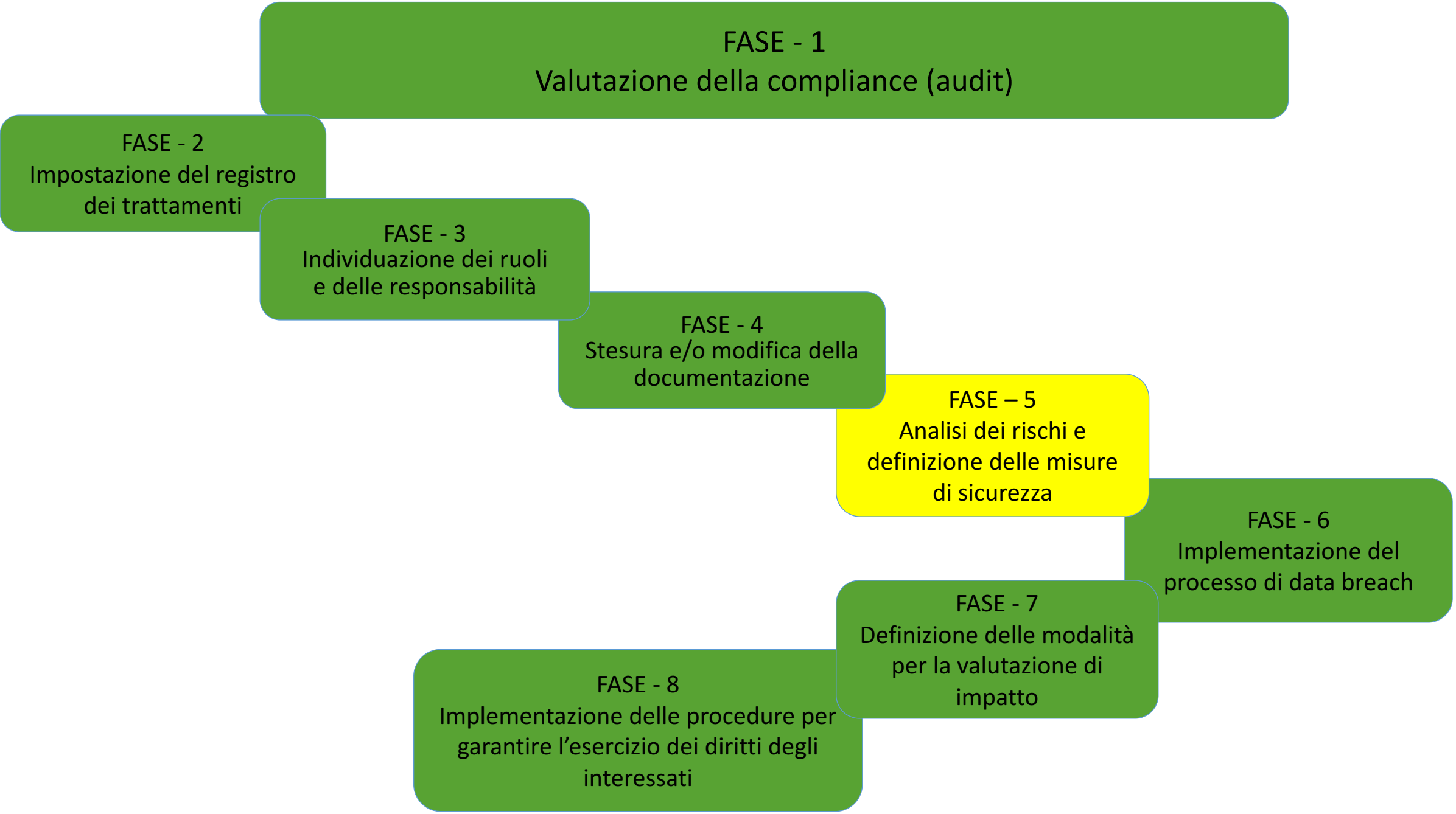
DPCM 3.12.2013 – Regole tecniche in materia di sistema di conservazione ca

Art. 12 – Sicurezza dei sistemi di conservazione

comma 1 – nelle pubbliche amministrazioni, il responsabile della conservazione predispone il piano della sicurezza del sistema di conservazione nel rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D.Lgs. 196/03 e dal disciplinare tecnico di cui all'allegato B)

comma 2 – i soggetti privati adeguano il sistema di conservazione a tali regole.

(dal 25 maggio 2018 si applica l'art. 32 del GDPR)


FASE - 1
Valutazione della compliance (audit)
FASE - 2
Impostazione del registro dei trattamenti
FASE - 3
Individuazione dei ruoli e delle responsabilità
FASE - 4
Stesura e/o modifica della documentazione
FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza
FASE - 6
Implementazione del processo di data breach
FASE - 7
Definizione delle modalità per la valutazione di impatto
FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase 5 - Analisi dei rischi e definizione delle misure di sicurezza

Come in qualsiasi processo di assessment efficace ed efficiente, non si può prescindere dalla mappatura dei rischi intesa come strumento di prevenzione e cura da possibili attacchi. Sarà assolutamente necessario (ex artt. 24 e 32 del GPPR):

- **individuare** i possibili ambiti di rischio che dovranno essere oggetto di valutazione;
- **definire** la ***metodologia di analisi dei rischi più adatta*** alla realtà organizzativa aziendale con particolare riferimento ai sistemi informativi;
- **analizzare** (per ogni trattamento o per trattamenti simili) sia i rischi connessi ai trattamenti effettuati senza l'utilizzo di strumenti elettronici, che quelli relativi alla configurazione dei sistemi informativi e ai software utilizzati;
- **censire** le attuali misure di sicurezza organizzative, fisiche e logiche;
- **definire** le misure di sicurezza necessarie a ridurre il rischio entro un livello di accettabilità (es. pseudonimizzazione, cifratura ecc.);
- **verificare** tutti gli applicativi adottati e da adottare e avviare politiche di controllo in linea con i principi di privacy by design e privacy by default (art. 25 GDPR);
- **documentare** le attività da sviluppare per rendere adeguata la propria organizzazione.

Sicurezza dei dati e dei sistemi: principi e garanzie

- riservatezza - garanzia che l'accesso ai dati sia consentito solo ai soggetti legittimati;
- integrità - garanzia che la modifica dei dati venga effettuata solo da parte dei soggetti autorizzati
- disponibilità - garanzia che il sistema e i dati siano accessibili e utilizzabili con continuità
- autenticità - garanzia che la fonte dei dati sia attendibile.

Sicurezza dei dati e dei sistemi: potenziali criticità

- comportamenti errati
- organizzazione carente
- logistica inadatta
- errori del software
- vulnerabilità hw e sw

Sicurezza dei dati e dei sistemi:
le diverse tipologie delle misure di sicurezza

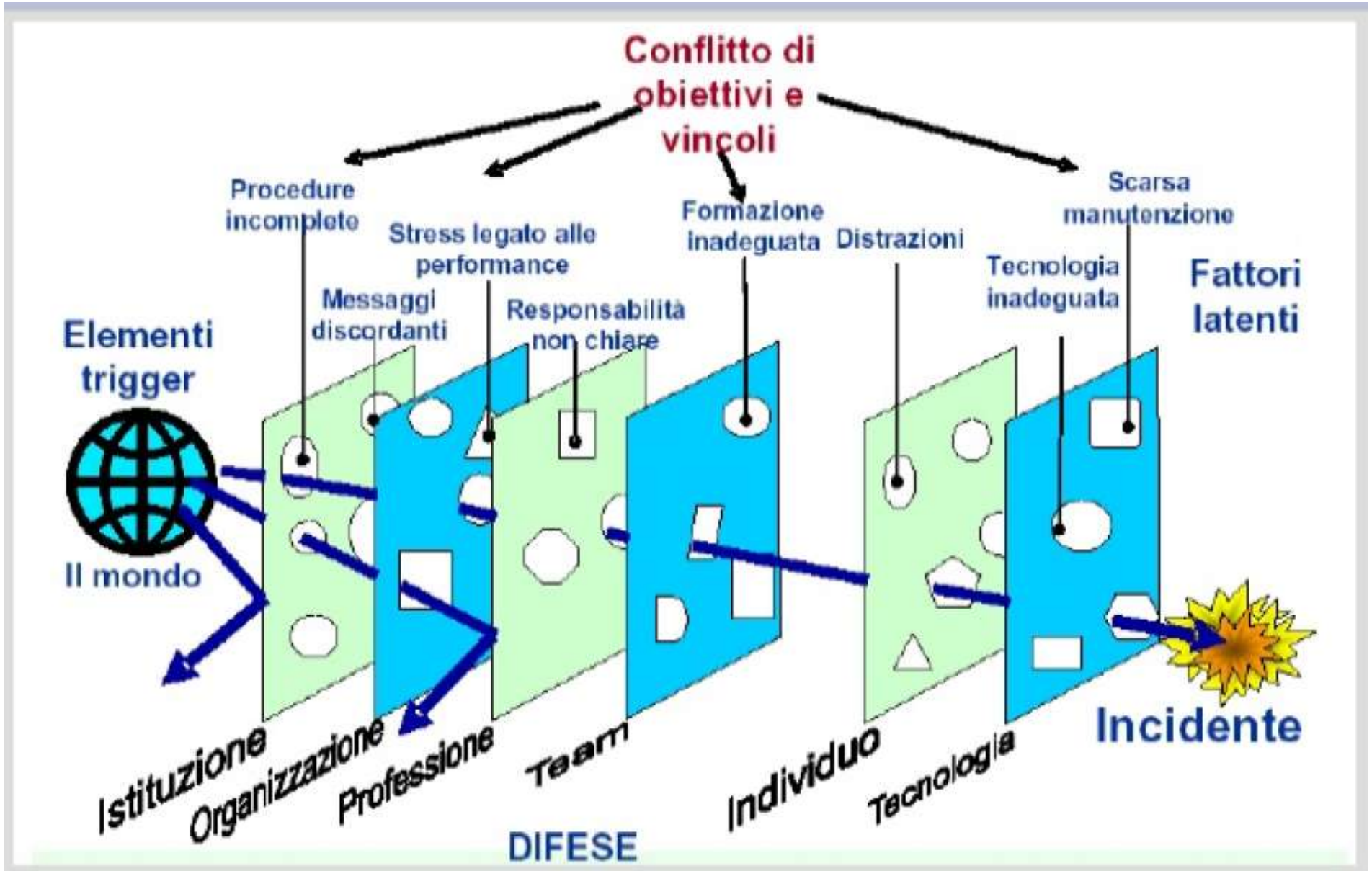
- misure di tipo organizzativo (es. designazione dei designati al coordinamento e autorizzati al trattamento, formazione, linee guida);

- misure di tipo fisico (es. ingressi controllati dei locali di custodia degli archivi e dei server);

- misure di tipo logico (es. sistema di autenticazione e di autorizzazione, antivirus, firewall, cifratura dei dati etc.)

ANALISI DEI RISCHI:

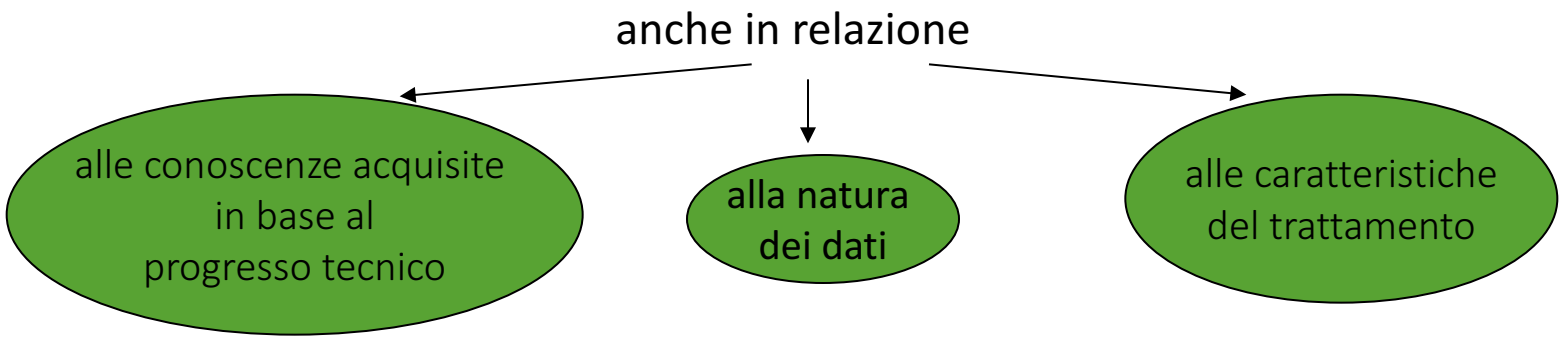
Il modello di Reason



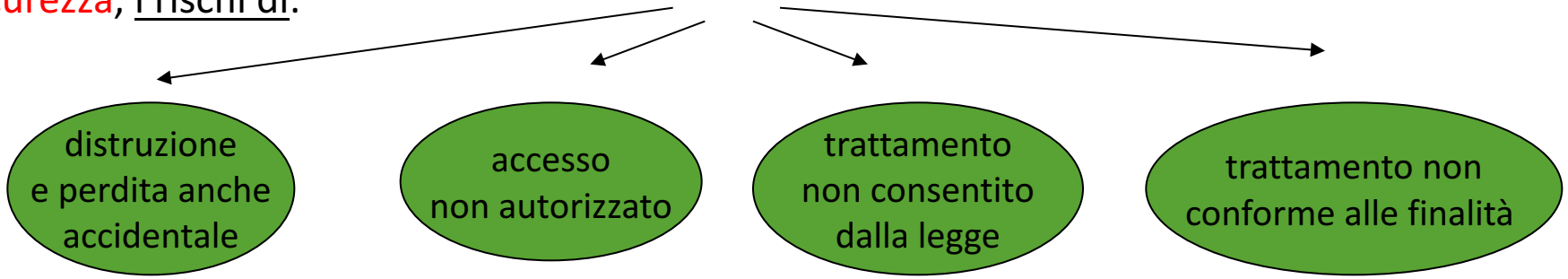
Misure di sicurezza nel (vecchio) D.Lgs. 196/03

Art. 31 del D.Lgs. 196/03 - Obblighi di sicurezza (oggi abrogato)

I dati personali oggetto di trattamento sono custoditi e controllati



in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di:



Art. 33 D.Lgs. 196/03 - Misure minime (oggi abrogato)

Nel quadro dei più generali obblighi di sicurezza di cui all'art. 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo, volte ad assicurare un livello minimo di protezione dei dati personali

Misure minime

I trattamenti sono consentiti solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

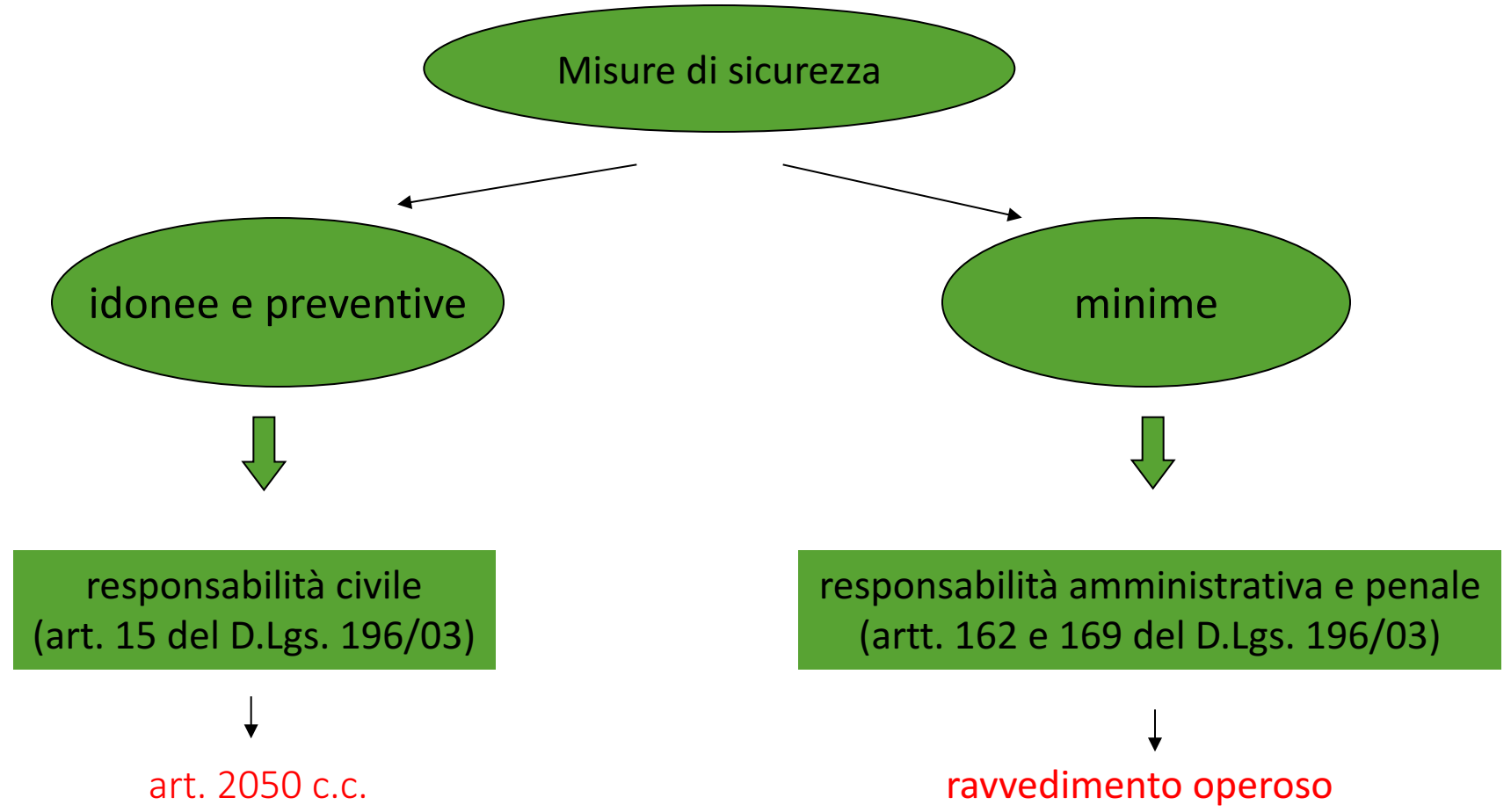
Art. 34 - trattamenti con strumenti elettronici

- autenticazione informatica e gestione delle credenziali di autenticazione;
- aggiornamento periodico dell'individuazione dell'ambito di trattamento;
- protezione degli strumenti elettronici;
- custodia di copie di sicurezza;
- tenuta di un aggiornato DPS;
- tecniche di cifratura per i dati sulla salute e la vita sessuale

Art. 35 - trattamenti senza l'ausilio di strumenti elettronici

- aggiornamento periodico dell'individuazione dell'ambito di trattamento;
- procedure per idonea custodia di atti e documenti affidati agli incaricati;
- conservazione di determinati atti in archivi ad accesso selezionato

Misure di sicurezza e responsabilità nel (vecchio) D.lgs. 196/03



Misure di sicurezza “necessarie”

Sono le misure prescritte dal Garante per la protezione dei dati personali ai sensi dell’art. 154, comma 1, lett.c) del D.Lgs. 196/03 con propri provvedimenti di carattere generale riguardanti particolari categorie di titolari e di attività di trattamento, oppure provvedimenti specifici nei confronti di singoli titolari

Misure di sicurezza nel GDPR

- considerando 39 …… I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

- art. 5.1 lett. f) - I dati personali sono 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»).

Responsabilità del titolare del trattamento (art. 24)

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.

Considerando 83

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Sicurezza del trattamento (art. 32 GDPR)

Il titolare e il responsabile del trattamento, tenuto conto:

- dello stato dell'arte e dei costi di attuazione
- della natura, dell'oggetto, del contesto e delle finalità perseguite dal trattamento
- dei rischi di varia probabilità e gravità per i diritti e e le libertà delle persone fisiche

mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Scalabilità e adeguatezza delle misure di sicurezza al caso concreto

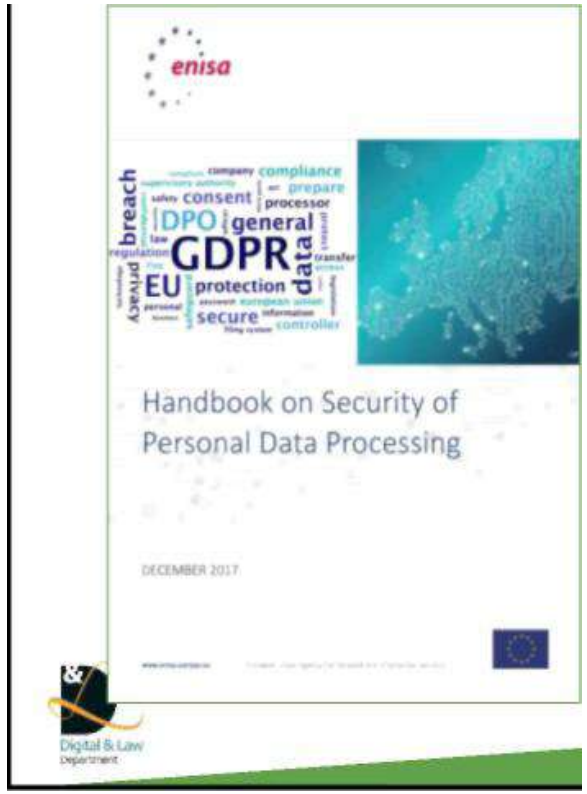
WP29, Opinione 3/2010, p. 13, § 45: “Da quanto precede risulta che nel determinare i tipi di azioni da attuare, non esistono alternative valide alle soluzioni “su misura”. Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. Un approccio uguale per tutti avrebbe il solo effetto di costringere i titolari del trattamento all’interno di strutture inadatte e si rivelerebbe quindi fallimentare”

Scalabilità e adeguatezza delle misure di sicurezza al caso concreto

Garante per la protezione dei dati personali - Guida all'applicazione del Regolamento europeo p. 27:

"Non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure 'minime' di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come dall'art. 32 del regolamento"

Handbook on security of personal data processing (ENISA)



Presenta e raccomanda una metodologia oggettiva per valutare il livello di rischio e le misure di sicurezza per i dati personali.
Presenta vari casi d'uso in diversi settori (HR, clienti, fornitori, marketing)

Dicembre 2017

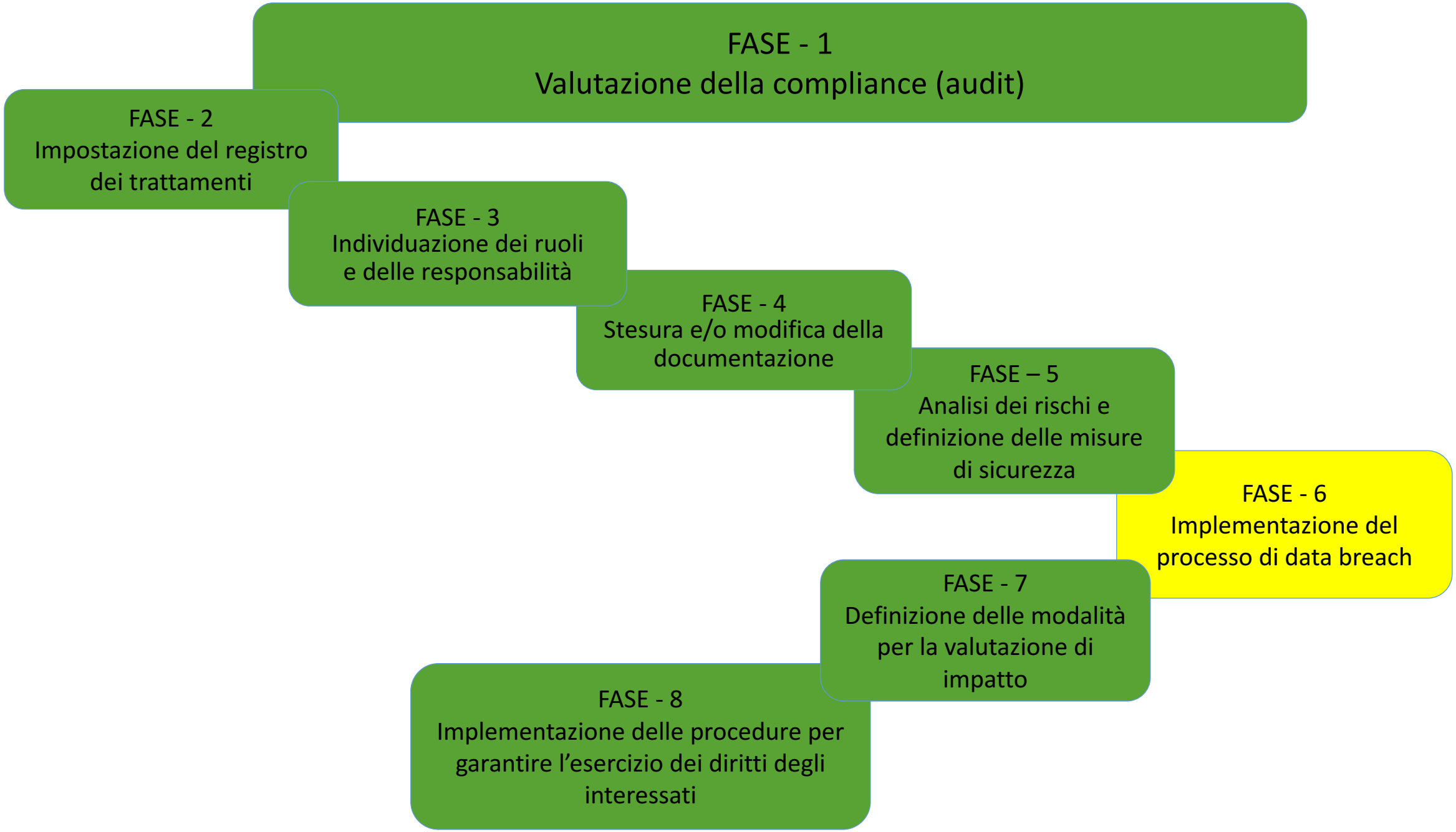
Digital & Law Department

Guidelines for SMEs on the security of personal data processing (ENISA)

Contiene utili suggerimenti per le Piccole e Medie imprese riguardanti le tecniche di valutazione dei rischi e le misure di sicurezza.

Dicembre 2016

Digital & Law Department


FASE - 1
Valutazione della compliance (audit)
FASE - 2
Impostazione del registro dei trattamenti
FASE - 3
Individuazione dei ruoli e delle responsabilità
FASE - 4
Stesura e/o modifica della documentazione
FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza
FASE - 6
Implementazione del processo di data breach
FASE - 7
Definizione delle modalità per la valutazione di impatto
FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase 6 - Implementazione del processo di data breach

In questa fase è opportuno concentrarsi anche sulle possibili violazioni nel trattamento di dati personali (artt. 33 e 34 GDPR), quindi:

- **definire e integrare le procedure di incident management** per la gestione dei data breach, in modo da ridurre il più possibile il termine che intercorre tra la violazione e il momento in cui ci si accorge della violazione (anche attraverso propri partner tecnologici)
- **implementare un sistema di file log** che consenta la raccolta di tutte le necessarie informazioni a supporto delle violazioni e delle opportune indagini sottostanti;
- **impostare il registro delle violazioni**;
- **definire la modulistica per le notificazioni** all'autorità di controllo (art. 33) e le comunicazioni agli interessati (art. 34).

Facebook violato, colpiti fino a 50 milioni di utenti

Quasi 50 milioni di account Facebook sono stati colpiti da un attacco hacker, le azioni della società sono scese del 3% dopo la diffusione della notizia

di **Giuditta Mosca**

28 SET, 2018

https://www.ilfattoquotidiano.it/2019/05/13/hacker-attaccano-siti-dellordine-degli-avvocati-la-sicurezza-

il Fatto Quotidiano.it

Hacker attaccano siti dell'Ordine degli avvocati. La sicurezza digitale in Italia è ancora vulnerabile

Tecnologia | 13 Maggio 2019

COMMENTI (35)

Più informazioni su: Anonymous, Innovazione Tecnologica, Ordine degli Avvocati

Andrea Lisi

Il collettivo **LulzSec_ITA**, impegnato negli ultimi giorni a violare i sistemi informatici degli Ordini degli avvocati di **Matera**, **Caltagirone** e **Piacenza** per poi arrivare a bucare 30mila Pec di avvocati romani, rivendica anche un attacco perpetrato ai danni del

CARICA L' APP

SIAE DALLA PARTE DI CHI CREA

CHI SIAMO

DIRITTO D'AUTORE · AUTORI ED EDITORI ·

ive & news

21.11.18
NEWS

Condividi

DATA BREACH DEL 2 NOVEMBRE 2018: COMUNICAZIONE DA SIAE

In seguito al data breach che si è verificato venerdì 2 novembre 2018 alle ore 23.34, SIAE ha eseguito le analisi e acquisito una chiara visione del problema legato alla violazione dei dati personali di alcuni utenti da parte di un gruppo anonimo di hacker.

La violazione è stata comunicata al Garante per la protezione dei dati entro i termini di legge e in seguito agli utenti interessati, oltre che denunciata presso le Autorità competenti. L'azione di hackeraggio ha colpito un numero inferiore al 2,5% degli utenti registrati ai nostri servizi online.

Per la Società Italiana degli Autori ed Editori la tutela dei propri associati e degli utenti è e resta prioritaria.

Per ulteriori informazioni è possibile contattare l'indirizzo email SiaeUfficioDataProtection@siae.it


```
[root@PC-Linux ~]# systemd-analyze
Startup finished in 10.940s (firmware) +
space) = 19.538s
graphical.target reached after 1.464s in
```


M5S: Garante privacy, istrutt
www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6700823
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
1997-2017: VENT'ANNI A TUTELA DI UN DIRITTO FONDAMENTALE
Home
L'Autorità
Provvedimenti e normativa
Attività e documenti
Stampa e comunicazione
Attività internazionali
Solo testo | Scegli la lingua: IT EN
DIRITTI E PREVENZIONE
> COME TUTELARE LA TUA PRIVACY
DOVERI E RESPONSABILITÀ
> COME TRATTARE I DATI PERSONALI DEGLI ALTRI
RICERCA
testo
docweb
inserisci chiave di ricerca
cerca
ricerca
avanzata
M5S: Garante privacy, istruttoria su attacco hacker. Aperta il 7 agosto con invio richiesta di informazioni
Ansa, 10 agosto 2017
SCHEDA
Doc-Web:
6700823
Data:
10/08/17
Tipologia:
Comunicato stampa
Ascolta
Stampa
PDF
Invia per mail
Condividi
M5S: Garante privacy, istruttoria su attacco hacker
Aperta il 7 agosto con invio richiesta di informazioni
(Ansa, 10 agosto 2017)
Il Garante della privacy segue da vicino la vicenda relativa all'attacco hacker subito on line dal Movimento 5 Stelle e già il 7 agosto ha aperto un'istruttoria in merito, inviando una richiesta di informazioni.
E' quanto si apprende dall'ufficio dell'Autorità, interpellato dall'Ansa sulla questione.
Le stesse fonti spiegano che ad istruttoria in corso non è possibile fornire ulteriori dettagli.
L'AUTORITÀ
Il Garante
Compiti del Garante
L'ufficio
PROVVEDIMENTI E NORMATIVA
Provvedimenti
Autorizzazioni generali
ATTIVITÀ E DOCUMENTI
Documenti e pubblicazioni
STAMPA E COMUNICAZIONE
Comunicati stampa
Newsletter
ATTIVITÀ INTERNAZIONALI
Cooperazione in ambito UE
17:00
04/10/2017

Attacco hacker al Pd fiorentino: online cellulari e indirizzi

E' stato rivendicato su Twitter dal gruppo AnonPlus: "La lista completa degli iscritti al Partito democratico di Firenze, con nomi, cognomi". C'è anche il vecchio numero di cellulare di Renzi. Indaga la polizia

di ERNESTO FERRARA

Lo leggo dopo

06 febbraio 2018

Tutto quello che c'è da sapere sull'attacco hacker al sito di incontri Ashley Madison

Pagamenti, indirizzi mail, numeri di telefono, ma anche le preferenze sessuali: sul deep web finiscono i dati di 32 milioni di fedifraghi

AP

Nato in Canada e presente in decine di Paesi con svariate migliaia di iscritti anche italiani, il sito di incontri molto gettonato negli Stati Uniti

TECNO

Privacy: Telecom sanzionata (ancora) per settemila utenze violate. Un rischio calcolato?

di Andrea Lisi | 19 maggio 2017

COMMENTI (41)

Più informazioni su: Garante della Privacy, Privacy, Telecom, Telecom Italia

Andrea Lisi
Esperto in diritto dell'informatica, Anorc

Uno degli aspetti più deteriori della mancanza di **una vera cultura digitale in Italia** è la tendenza comune a prendere un po' sottogamba **il diritto alla privacy**, anzi come sarebbe più corretto dire, diritto alla protezione dei **dati personali**. Di "privacy" in Italia si parla spesso e tante volte a sproposito, reclamandone la

MONDO
Catalogna, Puigdemont chiede tempo "Stop repressione e dialogo per 2 mesi" Ma non chiarisce sull'indipendenza

POLITICA
Sondaggi, il M5s primo partito. Il Pd insegue Lega e Forza Italia continuano a crescere

key4biz
dal 2002
9/3/2018 - S. Francesca Romana

LULZSEC ITALIA

Ascolta

Attacco hacker al Miur, pubblicati in rete migliaia di indirizzi di posta e password dei professori

L'azione rivendicata dal Gruppo Lulzsec Italia: "Salve Ministro dell'Istruzione, Valeria Fedeli, le diamo il benvenuto nell'arena". Poi le critiche alla riforma della Buona Scuola e all'alternanza scuola-lavoro.

di **Flavio Fabbri** | @FabbriFlav2 | 8 marzo 2018, ore 12:55

Video

Droni in passerella al posto delle modelle. L'efficace mossa di marketing di D&G

UBER DATA BREACH FROM 2016 AFFECTED 57 MILLION RIDERS AND DRIVERS

2017-11-21 NEWSBOT | ATTACK, DATA, NEWS, SECURITY

"Uber faced a data breach in 2016 that affected some 57 million customers, including both riders and drivers, revealing their names, email address and phone numbers" writes Minutes Ago Lucas for techcrunch.com. Uber did not report the incident to regulators or to affected customers, but instead paid $100,000 to "hackers" to get rid of the data in order to keep the breach under wraps, according to the report.The report says the attack occurred because attackers managed to gain login credentials for an Uber Amazon Web Services account using a private GitHub site maintained by Uber engineers.

Source: techcrunch.com

Attacco hacker a Uber: Dichiarazione Antonello Soro, Presidente dell'Autorità Garante per la privacy (22.11.2017)

"Non possiamo che esprimere forte preoccupazione per la violazione subita da Uber, tardivamente denunciata dalla società americana. Abbiamo aperto un'istruttoria e stiamo raccogliendo tutti gli elementi utili per valutare la portata del data breach e le azioni da intraprendere a tutela degli eventuali cittadini italiani coinvolti. Quello che certo colpisce, in una multinazionale digitale come Uber, è l'evidente insufficienza di adeguate misure di sicurezza a protezione dei dati e quello che sconcerta è la scarsa trasparenza nei confronti degli utenti sulla quale indagheremo".

Sezioni

Hot topics

Approfondimenti

Categorie

Big Data

Biometria

Cloud

Data Transfer

Droni

E-commerce

Finance & Insurance

Data breach del 2018 costa a British Airways una multa da 204 milioni

L'Information Commitioner's Office (ICO) – l'Autorità per la protezione dei dati del Regno Unito – ha **annunciato oggi l'intenzione di comminare una sanzione da 183 milioni di sterline** (204 milioni di Euro) che British Airways dovrà pagare perché ritenuta responsabile ai sensi del **GDPR** per il *data breach* occorso nel 2018.

A cavallo dell'estate dell'anno passato, la compagnia aerea britannica **aveva subito un cyberattacco che aveva coinvolto i dati personali di centinaia di migliaia di passeggeri**. Dopo un'indagine durata diversi mesi, si è acclarato che, per il periodo in cui l'attacco ha prodotto i suoi effetti, gli utenti del sito web di British Airways che erano regolarmente dirottati verso un sito fraudolento ed ora ammonta risulta circa 500.000 clienti i cui dati personali sono finiti nelle disponibilità degli hacker che architettato l'incursione. Tra le informazioni carpite ai passeggeri si annoverano credenziali di accesso a siti e app della compagnia, dati anagrafici, dati di contatto, prenotazioni e dettagli di viaggio e identificativi degli strumenti di pagamento utilizzati (soprattutto carte di credito con relativi codici di sicurezza).

British Airways nel settembre 2018 aveva notificato la violazione nei tempi stabiliti da GDPR (ossia, ex art. 33 del Regolamento entro 72 ore dal momento in cui ne è venuta a conoscenza) e si era fin da subito attivata per supportare i clienti esposti a potenziali danni. L'ICO oggi le riconosce anche di aver collaborato alle indagini di questi mesi e di aver implementato significative migliorie ai propri sistemi di protezione informatica. Ma tanto non è bastato alla compagnia per evitare che l'Autorità propendesse per una sanzione da record: l'ICO definisce "povere" le misure di protezione informativa al tempo in uso e intende punire in modo esemplare le svariate carenze di sicurezza che resero possibile una vera razzia di informazioni private relative a migliaia di persone di tutto il mondo (a tal proposito, per quanto ovvio, è bene ricordare che l'ICO funge da capofila per le restanti autorità nazionali secondo il principio "One Stop Shop" introdotto dall'art. 56 del GDPR).

Privacy addio, documenti medici gettati per strada e a disposizione di tutti

Un maxi archivio a cielo aperto con tanto di nomi, cognomi e trattamenti medici, per chiunque voglia conoscere i fatti degli altri. I fogli riportano l'intestazione del Centro di riabilitazione Il Carrobiolo di vicolo Scuole

di Marco Galvani

Ultimo aggiornamento il **14 maggio 2015 alle 11:03**

Condividi Tweet Invia tramite email

POTREBBE INTERESSARTI ANCHE

CRONACA

Rifiuti Roma, caos Ama. Il Cda si dimette in blocco

È un data breach anche questo?

Definizione di violazione di dati personali (art. 4.12 del GDPR)

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;

L’obbligo di notificare gli eventi di data breach non è una novità assoluta

I PROVVEDIMENTI CITATI NELL'INFOGRAFICA

- Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) 4 aprile 2013

- Provvedimento generale prescrittivo in tema di biometria 12 novembre 2014

- Linee guida in materia di Dossier sanitario 4 giugno 2015

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche 2 luglio 2015

Notifica e comunicazione dei data breach

- artt. 33 e 34
- considerando da 85 a 88
- Linee guida del 6 febbraio 2018 (WP250)

Quando è necessario effettuare la notifica di una violazione dei dati personali all'autorità di controllo? (art. 33)

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.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Comunicazione di una violazione dei dati personali all'interessato (art. 34)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

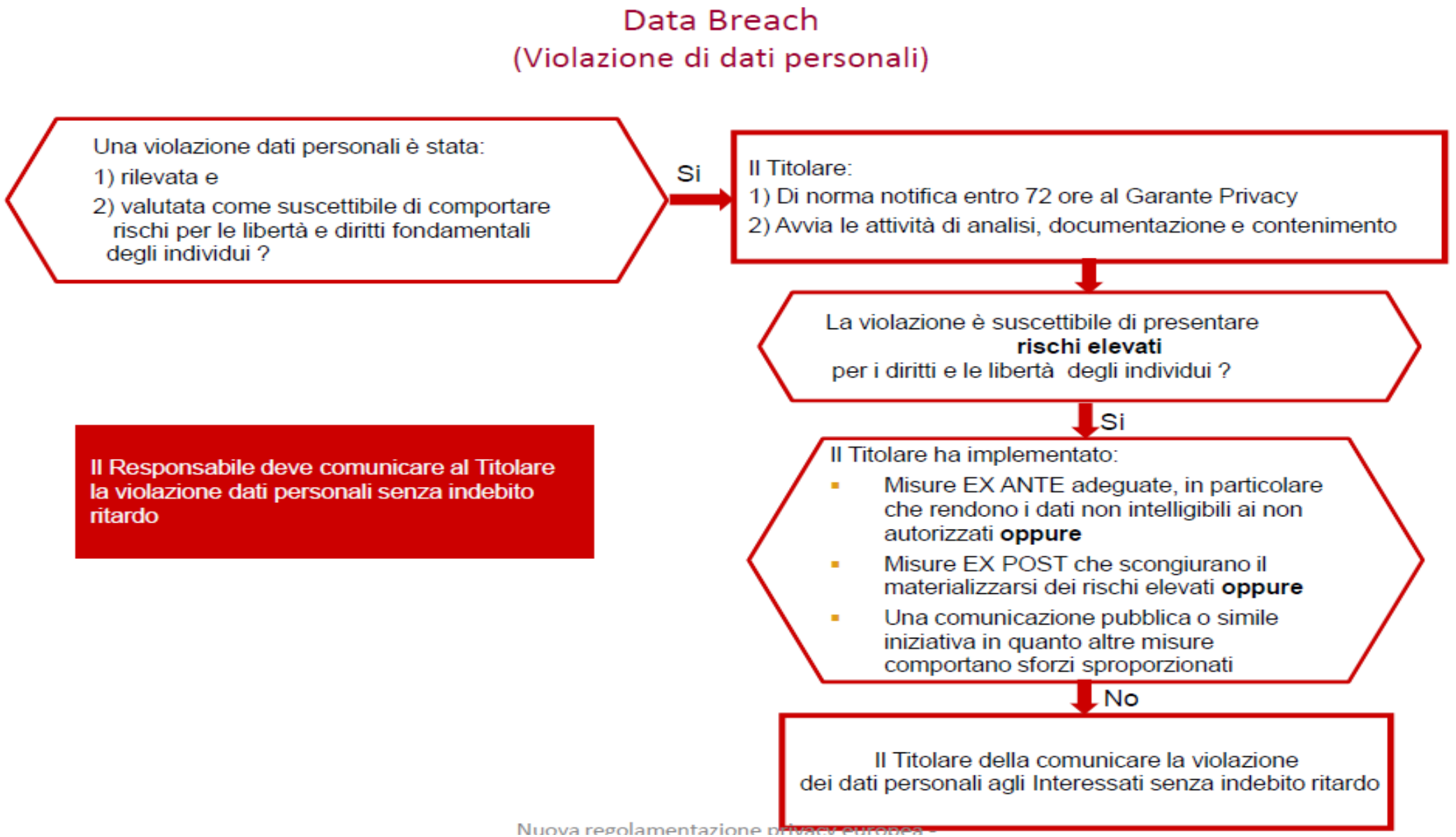
2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno:
   - il nome e i dati di contatto del DPO o altri soggetti dai quali poter ottenere ulteriori informazioni;
   - la descrizione delle probabili conseguenze della violazione;
   - le misure adottate per porvi rimedio e attenuarne i possibili effetti negativi;

Casi per i quali la comunicazione di una violazione dei dati personali all'interessato non è dovuta (art. 34.3)

- il titolare del trattamento aveva adottato misure tecniche ed organizzative adeguate per proteggere i dati personali oggetto della violazione (es. pseudonimizzazione o cifratura);
- il titolare del trattamento ha successivamente adottato misure in grado di scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Esempio


Data Breach
(Violazione di dati personali)
Una violazione dati personali è stata:
1) rilevata e
2) valutata come suscettibile di comportare rischi per le libertà e diritti fondamentali degli individui ?
Si
Il Titolare:
1) Di norma notifica entro 72 ore al Garante Privacy
2) Avvia le attività di analisi, documentazione e contenimento
La violazione è suscettibile di presentare rischi elevati per i diritti e le libertà degli individui ?
Si
Il Titolare ha implementato:
Misure EX ANTE adeguate, in particolare che rendono i dati non intelligibili ai non autorizzati oppure
Misure EX POST che scongiurano il materializzarsi dei rischi elevati oppure
Una comunicazione pubblica o simile iniziativa in quanto altre misure comportano sforzi sproporzionati
No
Il Titolare della comunicare la violazione dei dati personali agli Interessati senza indebito ritardo
Il Responsabile deve comunicare al Titolare la violazione dati personali senza indebito ritardo

Come valutare il rischio conseguente a un “data breach” ?

Secondo il WP29, i fattori che devono essere presi in considerazione per valutare il livello del rischio - e, quindi, la decisione se effettuare o meno la notifica e la comunicazione - sono:

- Il **tipo di violazione e la natura dei dati violati** (es. violazione di riservatezza, di accessibilità o di integrità dei dati; dati sanitari, documenti di identità o numeri di carte di credito);
- la **facilità con cui potrebbero essere identificati gli interessati** (es. l’aggressione riguarda dati identificativi o dati personali non direttamente identificativi?; era previsto l’utilizzo di tecniche di pseudonimizzazione o crittografia?);
- la **gravità delle conseguenze sugli individui in termini di potenziali danni** (es. i dati sono stati inviati erroneamente a un fornitore di fiducia o sono stati sottratti da un terzo sconosciuto);
- **speciali caratteristiche e numero degli individui interessati** (es. bambini o anziani; violazione massiccia o individuale);
- **particolari caratteristiche del titolare** (es. ambito di attività economico o sanitario; contatto frequente con dati sensibili).

Obbligo di documentazione (art. 33.5)

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Cosa è cambiato dal 25 maggio 2018?

- tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo";

- la notifica all'autorità di controllo dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati, che spetta al titolare.

- tutti i titolari dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative conseguenze e i provvedimenti adottati (in caso di accertamento la documentazione va fornita all'autorità di controllo);

REGISTRO DELLE VIOLAZIONI

Organizzazione:	**Data:**

Nr.	I dettagli della violazione							Conseguenze della violazione	Le misure adottate o da adottare			
	Data di violazione	No. di persone colpite	Area / Processo interessato	Descrizione della violazione	Come si è venuto a conoscenza della violazione	Descrizione dei dati	Natura della violazione (scegli più pertinente)		Tutti gli interessati sono stati informati?	Azioni correttive	Altri soggetti informati	Data di la prima notifica al Garante

Contenuti minimi della notifica di una violazione dei dati personali all'autorità di controllo (art. 33.3)

- descrivere la natura della violazione dei dati personali nonché, quando possibile, le categorie e il numero approssimativo di interessati coinvolti, le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o che si propone di adottare per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire le suddette informazioni contestualmente, le stesse possono essere fornite in fasi successive senza ingiustificato ritardo.

Modello di comunicazione al Garante dei data breach

- Identità del titolare e coordinate di contatto della persona fisica addetta alla comunicazione;
- natura della comunicazione (nuova comunicazione, integrazione);
- breve descrizione della violazione;
- quando si è verificata la violazione? (data, dal..al.., ancora in corso)
- dove è avvenuta la violazione? (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili);
- tipo di violazione (lettura, copia, alterazione, cancellazione, furto, altro);
- dispositivo oggetto della violazione (computer, rete, dispositivo mobile, file o parte di un file, strumento di backup, documento cartaceo, altro)

Modello di comunicazione al Garante dei data breach

- sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;

- numero di interessati coinvolti dalla violazione;

- natura dei dati oggetto di violazione (anagrafici, numeri di telefono, indirizzi di posta elettronica, dati di accesso e di identificazione, dati di pagamento, dati sensibili e giudiziari, altro)

Modello di comunicazione al Garante dei data breach

- livello di gravità della violazione dei dati personali secondo la valutazione del titolare (basso/trascurabile, medio, alto, molto alto);
- misure tecniche e organizzative applicate ai dati oggetto di violazione;
- la violazione è stata comunicata agli interessati? (si, il…, no, perché);
- contenuto della comunicazione resa agli interessati e canale utilizzato per fornirla;
- misure tecniche e organizzative adottate per contenere la violazione dei dati e prevenire simili violazioni future;
- La violazione coinvolge interessati che si trovano in altri Paesi UE? Se si la comunicazione è stata effettuata alle competenti autorità degli altri Paesi UE?

Recommendation for a methodology of the assessment of severity of personal data breach (ENISA)

Presenta e raccomanda una metodologia
oggettiva per valutare il livello di gravità di una violazione
di dati personali (data breach).
Il calcolo dell'indice si basa sui seguenti tre fattori:
- contesto
- facilità di identificazione
- circostanze della violazione

Dicembre 2013

Le linee guida del Garante spagnolo

L'AEPD, autorità garante spagnola, ha diffuso una guida a supporto della decisione di notificare i Data Breach, che dovrebbe basarsi sui seguenti tre parametri:

1. Volume dei dati violati
2. Tipologia di dati violati
3. Impatto della violazione

i quali sono valutati attraverso l'attribuzione di un valore numerico in linea con i seguenti criteri:

VOLUME DEI DATI VIOLATI

Numero di record di identificazione completi	*Punteggio attribuito*
Meno di 100	1
Tra 100 e 1.000	2
Tra 1.000 e 100.000	3
Tra 100.000 e 1.000.000	4
Oltre 1.000.000	5

TIPOLOGIA DI DATI VIOLATI

Tipologia di dato personale	*Punteggio attribuito*
Dato personale comune	1
Dato sensibile/particolare	2

IMPATTO DELLA VIOLAZIONE

Grado di divulgazione	*Punteggio attribuito*
Nessuna divulgazione	2
Interna all'organizzazione, controllata	4
Esterna all'organizzazione	6
Pubblica (es. divulgazione su Internet)	8
Sconosciuta	10

Fonte: https://www.studiolegalestefanelli.it

Procedura per la rilevazione, valutazione e gestione dei data breach

- Definizioni e normativa di riferimento
- Compiti e responsabilità e istituzione di un “team di risposta” che valuta:
  - le segnalazioni ricevute sia dall’interno che dall’esterno e mantiene aggiornato il registro delle violazioni;
  - il rischio sui diritti e le libertà fondamentali degli interessati per ogni violazione segnalata e sottopone al Titolare i provvedimenti conseguenti;
- Definizione delle modalità con le quali devono essere segnalate le violazioni al team di risposta;
- Definizione dei criteri con i quali il team di risposta deve valutare il livello del rischio per i diritti e le libertà degli interessati (probabilità x gravità) e relativa tabella a supporto della decisione se effettuare o meno la notifica all’Autorità Garante e la comunicazione agli interessati;
- Verifica da parte del team di risposta delle contromisure adottate per porre rimedio alla violazione, nonché per attenuarne i possibili effetti negativi sugli interessati (cfr. art. 34.3.b).

FASE - 1
Valutazione della compliance (audit)

FASE - 2
Impostazione del registro dei trattamenti

FASE - 3
Individuazione dei ruoli e delle responsabilità

FASE - 4
Stesura e/o modifica della documentazione

FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza

FASE - 6
Implementazione del processo di data breach

FASE - 7
Definizione delle modalità per la valutazione di impatto

FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

Fase 7 - Definizione delle modalità per l'effettuazione della valutazione di impatto

Il principio di accountability non prevede più la verifica preliminare da parte dell'autorità di controllo (in passato prevista dall'art. 17 - oggi abrogato - del nostro Codice), ma diviene indispensabile (ex art. 35 del GDPR):

- **individuare**, i trattamenti per i quali è necessario effettuare **la valutazione d'impatto**;
- **individuare la metodologia più appropriata** da utilizzare per la valutazione d'impatto;
- **effettuare la valutazione d'impatto** per singoli trattamenti (o per gruppi simili di trattamenti che presentino rischi analoghi) nonché le necessarie misure tecniche ed organizzative per attenuarli;
- **predisporre e conservare la documentazione** relativa alla DPIA (Data Privacy Impact Assessment);
- **definire le modalità per il monitoraggio e l'eventuale revisione** della DPIA.

Ovvio anche che, nel momento in cui le nostre azioni ci sembrano non bastare per minimizzare i rischi di carattere elevato evidenziati nella DPIA, allora si potrà (eccezionalmente) avviare un **processo di consultazione preventiva con l'Authority** (art. 36 GDPR).

Valutazione d’impatto sulla protezione dei dati personali (DPIA)

- artt. 35 e 36
- considerando 84 e da 89 a 95
- linee guida del 4 ottobre 2017 (WP248)

Considerando 84

Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

Valutazione d'impatto sulla protezione dei dati (art. 35.1 e .2)

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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

per lo svolgimento della valutazione d'impatto il titolare si deve consultare con il DPO

Casi per i quali la valutazione d'impatto sulla protezione dei dati è obbligatoria (art. 35.3)

La valutazione d'impatto sulla protezione dei dati è necessaria in particolare nei casi seguenti:

- 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;
- trattamento, su larga scala, di dati sensibili e giudiziari;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'autorità di controllo deve redigere un elenco delle tipologie di trattamento per le quali è necessario effettuare la valutazione e può redigere anche un elenco per le quali non è necessario (entrambi gli elenchi saranno resi pubblici)

Contenuti minimi della valutazione d'impatto (art. 35.7)

- descrizione dei trattamenti e delle finalità perseguite, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

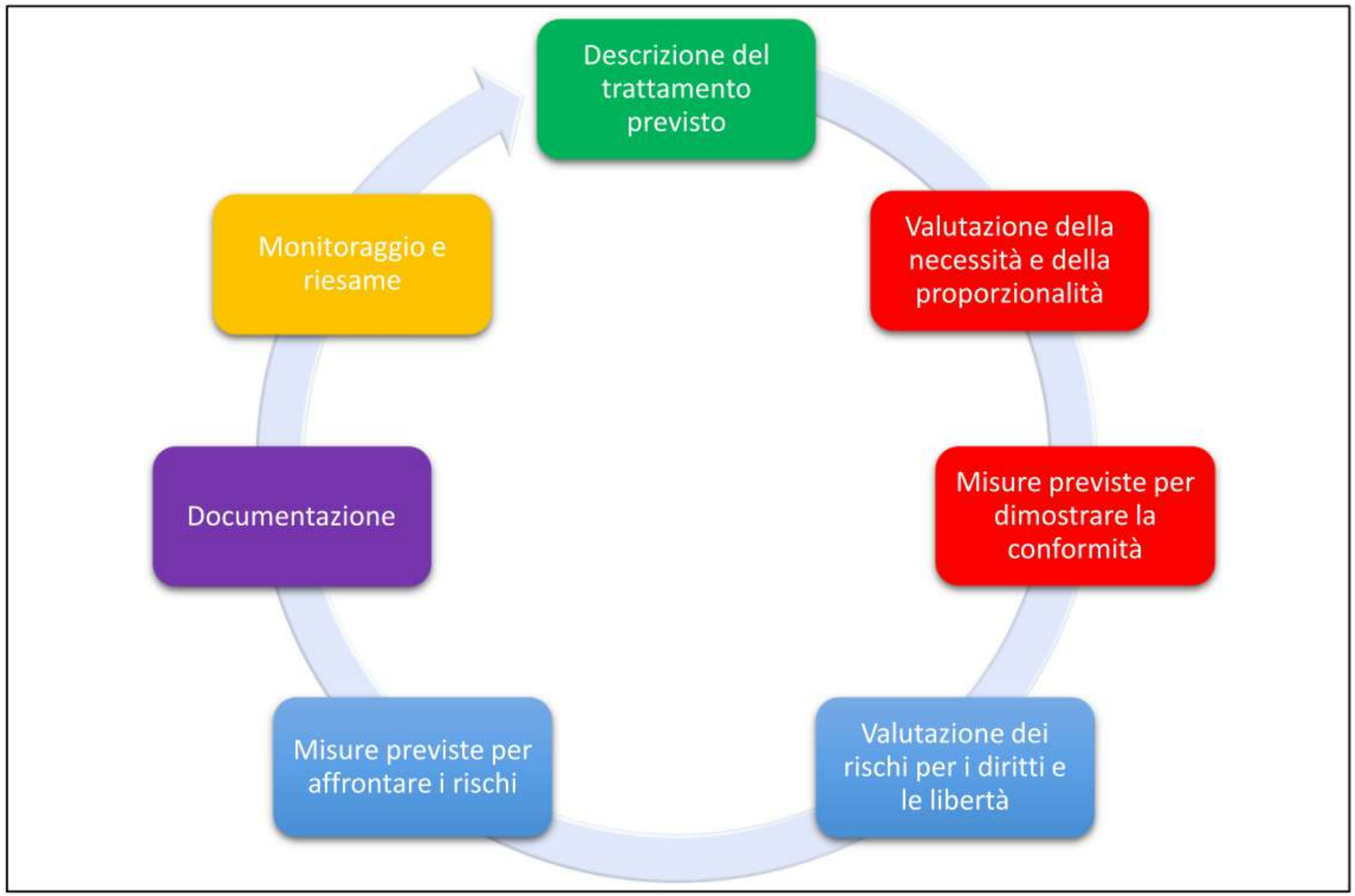
- valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguite;

- valutazione dei rischi per i diritti e le libertà degli interessati;

- 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 regolamento.

Valutazione d’impatto sulla protezione dei dati (DPIA).

Come effettuarla?



Consultazione preventiva (art. 36)

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un rischio residuo elevato, il titolare deve consultare l'autorità di controllo, fornendo le seguenti informazioni:

a) le rispettive responsabilità del titolare, degli eventuali contitolari e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

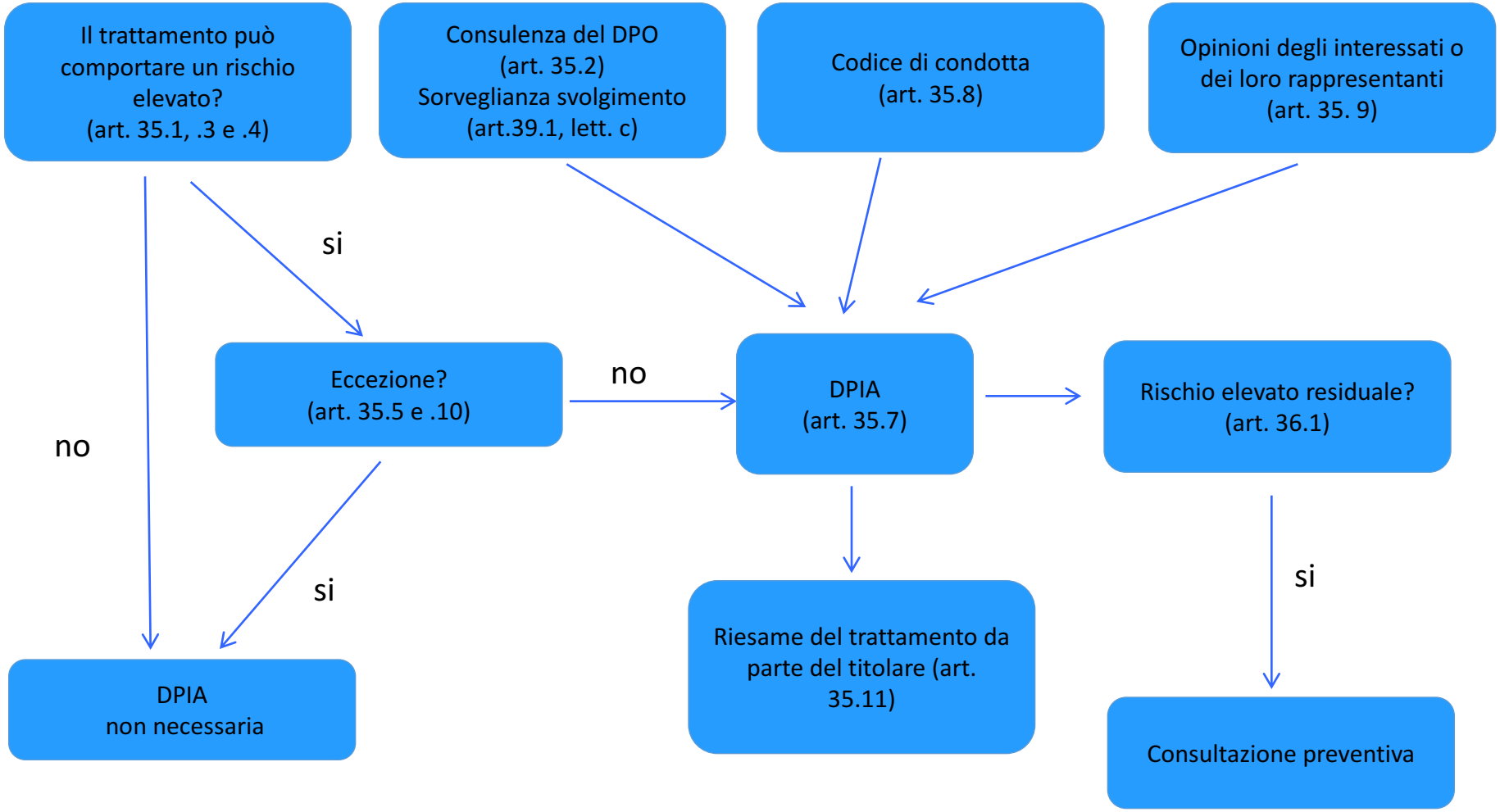
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) i dati di contatto del DPO, se designato;

e) la valutazione d'impatto sulla protezione dei dati;

f) ogni altra informazione richiesta dall'autorità di controllo.

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



Linee guida del Wp 29 sulla valutazione d'impatto del 4/4/2017 emendate in data 4/10/2017

- La valutazione d'impatto è una procedura che permette di realizzare e dimostrare la conformità con le norme;
- Per rischio si intende uno scenario descrittivo di un evento e delle relative conseguenze, che devono essere stimate in termini di gravità e probabilità;
- i titolari devono valutare in modo continuativo i rischi insiti nei propri trattamenti così da individuare le situazioni in cui una determinata tipologia di trattamenti può presentare un rischio elevato;
- Una DPIA può riguardare un singolo trattamento, tuttavia è possibile utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi;

Linee guida del Wp 29 sulla valutazione d'impatto del 4/4/2017 emendate in data 4/10/2017

- Una DPIA può rivelarsi utile anche per valutare l'impatto di un nuovo dispositivo hardware o software (privacy by design);
- Per stabilire se un trattamento deve essere soggetto alla valutazione d'impatto, è opportuno prendere in esame i seguenti criteri:
  - trattamenti valutativi o di scoring, compresa la profilazione e le attività predittive, in particolare a partire da aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
  - trattamenti automatizzati finalizzati ad assumere decisioni che producono significativi effetti giuridici sugli interessati;

Linee guida del Wp 29 sulla valutazione d'impatto del 4/4/2017 emendate in data 4/10/2017

- trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- trattamenti su larga scala di dati sensibili e giudiziari;
- combinazione o raffronto di insiemi di dati personali derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- trattamenti relativi a dati di interessati che si trovano in una condizione di non poter disporre del potere di acconsentire o di opporsi con facilità al trattamento dei propri dati (es. minori, dipendenti, pazienti, anziani, richiedenti asilo ecc.);

Linee guida del Wp 29 sulla valutazione d'impatto del 4/4/2017 emendate in data 4/10/2017

- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. controllo accessi mediante l'utilizzo di dati biometrici);
- trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca)

Secondo il WP 29, nella maggioranza dei casi, quando un trattamento soddisfa due o più dei criteri sopra indicati, è necessario condurre una DPIA

Linee guida del Wp 29 sulla valutazione d'impatto del 4/4/2017 emendate in data 4/10/2017

- non è necessario condurre una DPIA per i trattamenti in corso che sono stati oggetto di una verifica dell'autorità di controllo, purchè gli stessi proseguano con le stesse modalità oggetto di tale verifica e non siano intervenute variazioni dei rischi;
- pur non essendo obbligatorio pubblicare una DPIA, il WP 29 suggerisce che pubblicarne una sintesi può favorire un rapporto fiduciario con gli interessati, dando prova di un approccio responsabile e trasparente;
- Il titolare ha l'obbligo di conservare la documentazione della DPIA e di riesaminare la stessa periodicamente.

Allegato 2 delle linee guida del Wp 29 sul DPIA

Descrizione funzionale e sistematica del trattamento

- natura, ambito di applicazione, contesto, finalità e base giuridica del trattamento ;
- tipologia dati personali;
- destinatari (flusso interno ed esterno dei dati)
- periodo di conservazione;
- Strumenti del trattamento (hardware, software, reti, persone, trattamento cartaceo o trasmissione cartacea).

Allegato 2 delle linee guida del Wp 29 sul DPIA

Valutazione della necessità e proporzionalità del trattamento

Indicare le misure previste per l'osservanza del GDPR con riferimento in particolare:

- all'attuazione dei principi del trattamento [art. 5]
- al rispetto delle basi giuridiche [art. 6]
- al rispetto dei diritti degli interessati [artt. da 12 a 22]
- all'allocazione dei ruoli: rapporti con i contitolari [art. 26] e i responsabili del trattamento [art. 28]
- alle garanzie adottate per i trasferimenti extra-UE [capo V]
- all'eventuale consultazione preventiva [art. 36]

Allegato 2 delle linee guida del Wp 29 sul DPIA

Individuazione e valutazione dei rischi per i diritti e le libertà degli interessati e conseguente determinazione delle misure adeguate

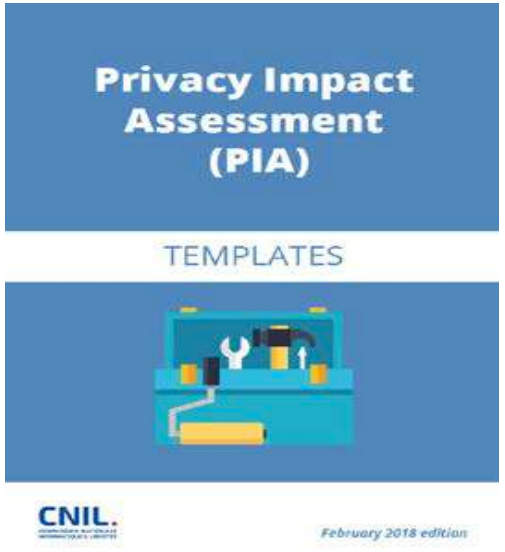
Per ciascun rischio (accesso illegittimo, modifica indesiderata e perdita dei dati) individuare:

- le fonti, la natura, la particolarità e la gravità;
- gli impatti potenziali per i diritti e le libertà degli interessati;
- le minacce che potrebbero determinare il rischio;
- la stima della probabilità e la gravità del rischio;
- le misure previste per l'elisione/mitigazione dei rischi individuati.

Un’applicazione utile

Questo è il link alla pagina del sito del Cnil che descrive le funzionalità del software e consente di scaricarlo
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
Questo, invece, è il file eseguibile per Windows (32 e 64 bits)
https://github.com/LINCnil/pia-app/releases/download/1.5.0/PIA-Setup-1.5.0.exe

Le tre guide del CNIL a supporto dell'effettuazione di un DPIA

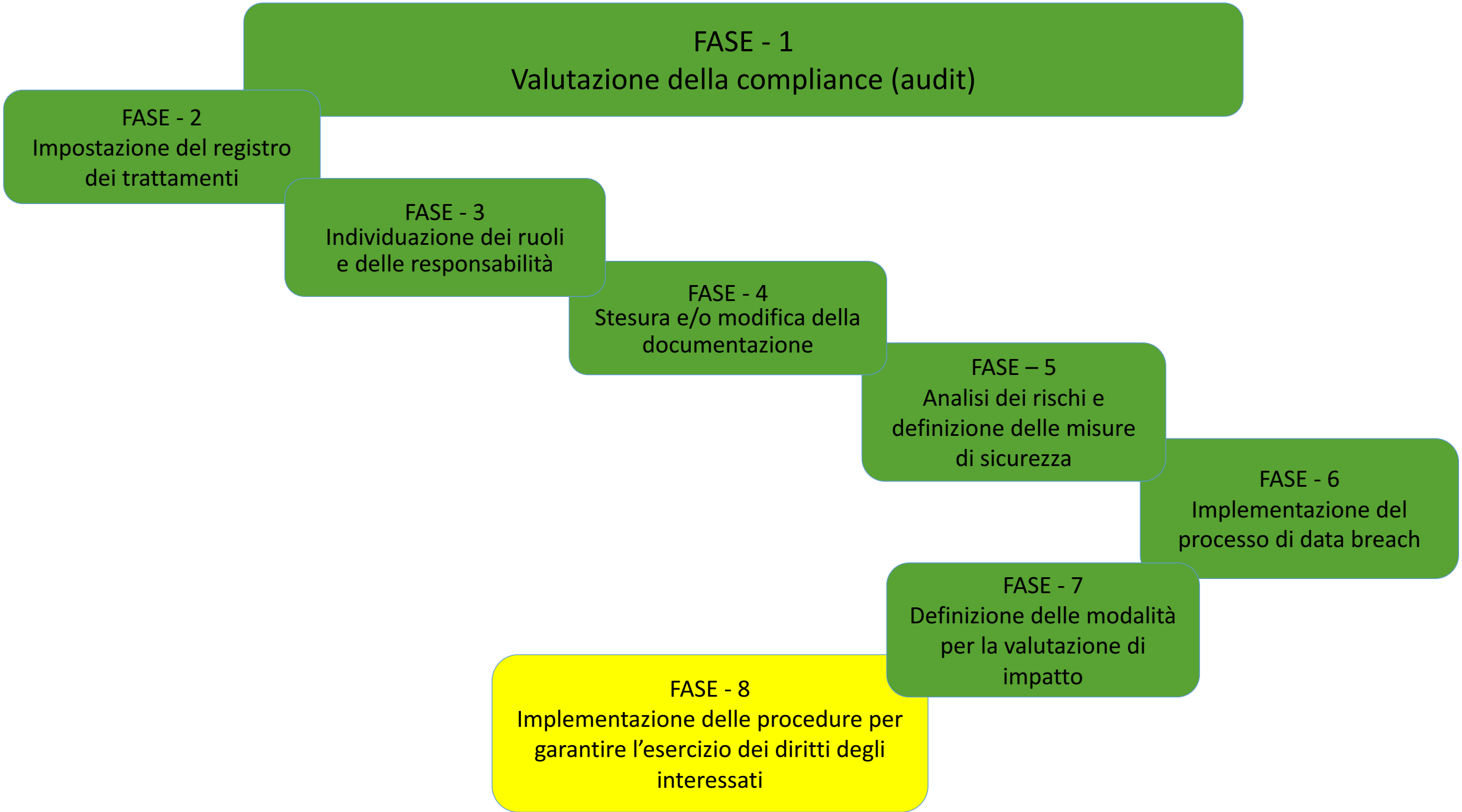


Methodology: basata sul rispetto dei principi applicabili al trattamento dei dati personali, nonché sull'analisi e la gestione dei rischi per i diritti e le libertà fondamentali degli interessati;
Templates: modelli da utilizzare per formalizzare le attività di analisi del contesto, della necessità e proporzionalità del trattamento, dei rischi e per la validazione del DPIA;
Knowledge bases: elenco di best practices e di misure di sicurezza organizzative e tecniche da adottare per mitigare i rischi

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati

- ✓ Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell’art. 35, comma 4, del Regolamento (UE) n. 2016/679 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018)

- ✓ ALLEGATO 1 - elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d’impatto


FASE - 1
Valutazione della compliance (audit)
FASE - 2
Impostazione del registro dei trattamenti
FASE - 3
Individuazione dei ruoli e delle responsabilità
FASE - 4
Stesura e/o modifica della documentazione
FASE – 5
Analisi dei rischi e definizione delle misure di sicurezza
FASE - 6
Implementazione del processo di data breach
FASE - 7
Definizione delle modalità per la valutazione di impatto
FASE - 8
Implementazione delle procedure per garantire l'esercizio dei diritti degli interessati

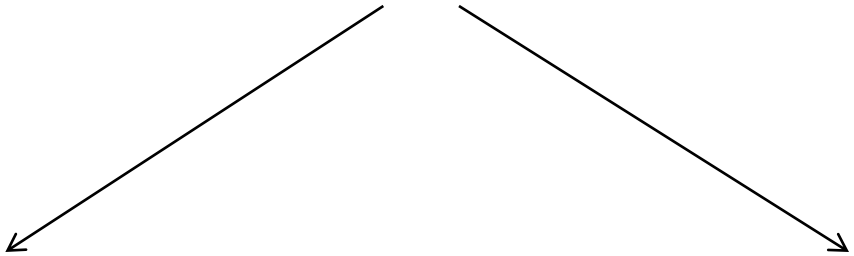
Fase 8 - Definizione delle procedure per garantire l'esercizio dei diritti degli interessati

Considerato che il GDPR ha reso più cogenti gli obblighi incombenti sul titolare, rafforzando il contesto di garanzie e procedure da osservare nel rapporto con gli interessati, è necessario:

- ✓ implementare le **procedure finalizzate ad agevolare l'esercizio dei diritti** da parte degli interessati;
- ✓ adottare **le misure organizzative e tecniche che consentano di rispettare i termini** previsti dall'art. 12 del GDPR;
- ✓ definire le **politiche di data retention**;

		Registro delle richieste relative all'esercizio dei diritti delle persone				
Organizzazione:						**Anno:**
No.	**Elementi di riferimento della richiesta**				**Accettata**	
	Data istanza	**Soggetto richiedente**	**Motivazione istanza**	**Tipo spedizione**	**Respinta**	Risposto in data

I diritti dell'interessato



Diritti conoscitivi

- ✓ diritto all'informativa (artt. 13 e 14)
- ✓ diritto di accesso (art. 15)
- ✓ diritto alla comunicazione di una violazione di dati (art. 34)

Diritti di controllo

- ✓ diritto di rettifica e di integrazione (art. 16)
- ✓ diritto di cancellazione/oblio (art. 17)
- ✓ diritto di limitazione (art. 18)
- ✓ diritto alla portabilità dei dati (art. 20)
- ✓ diritto di opposizione (art. 21)
- ✓ diritto a non subire decisioni basate unicamente su trattamenti automatizzati (art. 22)

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12)

Il regolamento ha rafforzato il contesto complessivo di garanzie e procedure da osservare nello svolgimento del trattamento e nel rapporto con l'interessato, rendendo più precisi e cogenti gli obblighi incombenti sul titolare;

Il titolare deve adottare misure appropriate per:

[.....]

agevolare l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22;

La violazione delle disposizioni relative ai diritti degli interessati, contenute negli articoli da 12 a 22, è soggetta a sanzioni amministrative pecuniarie fino a 20 milioni di euro o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore

Considerando 59

- E’ opportuno prevedere modalità volte ad agevolare l’esercizio, da parte dell’interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l’accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione.
- Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici.
- Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell’interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (febbraio 2018)

MODALITA' PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

cosa cambia

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità (il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta).

- Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Può essere dato oralmente solo se così richiede l'interessato stesso.

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (febbraio 2018)

MODALITA' PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Raccomandazioni

- Il titolare del trattamento deve adottare ogni idonea misura tecnica ed organizzativa finalizzata ad agevolare l'esercizio dei diritti da parte dell'interessato. Benchè sia il solo titolare a dover dare riscontro, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (cfr. art. 28, paragrafo 3, lett. e)

- Utili indicazioni sono contenute in alcuni provvedimenti del Garante quali ad esempio doc.web n. 1449401(dati sanitari) e doc.web 1290018 (dati telematici).

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (febbraio 2018)

Raccomandazioni

- diritto di accesso: consentire agli interessati, se possibile, di consultare direttamente i propri dati personali direttamente da remoto in modo sicuro (cfr. considerando 68);
- Diritto di cancellazione (diritto all'oblio): adottare misure ragionevoli per informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati (cfr. art. 17, paragrafo 2);
- Diritto di limitazione: prevedere nei propri sistemi informativi (elettronici o meno) misure idonee per escludere ogni operazione di trattamento diversa dalla conservazione;
- Diritto alla portabilità: adottare le misure necessarie a produrre i dati richiesti in un formato interoperabile secondo le indicazioni delle linee guida del WP29

Limitazioni (art. 23)

Al fine di salvaguardare alcuni particolari interessi di carattere generale o di proteggere i diritti e le libertà altrui (cfr. paragrafo 1 dell'art. 23 del GDPR), il diritto dell'UE o degli Stati membri può limitare la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'art. 5;

- Art. 2-undecies del D.Lgs. 196/03 introdotto dal D.Lgs. 101/2018 (Limitazioni ai diritti dell'interessato)

- Art. 2-duodecies del D.Lgs. 196/03 introdotto dal D.Lgs. 101/2018 (Limitazioni per ragioni di giustizia)

Art. 2-terdecies del D.Lgs. 196/03 introdotto dal D.Lgs. 101/2018
(Diritti riguardanti le persone decedute)

- I diritti di cui agli articoli da 15 a 22 del GDPR, riferiti ai dati personali riconducibili a persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

- Il predetto esercizio non è ammesso, oltre che nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare (revocabile o modificabile);

- Il divieto non può comunque produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dal decesso dell'interessato, nonché del diritto di difendere in giudizio i propri interessi.

La formazione dei soggetti autorizzati

Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. 196/03)

Il punto 19 prevedeva che il DPS dovesse contenere, tra le altre, idonee informazioni riguardo:

"la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare".

abrogato dalla legge 4 aprile 2012, n. 35

La centralità della formazione nel GDPR

- ✓ l'art. 29 del GDPR prevede che *"il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento …".*

- ✓ l'art. 32, paragrafo 4, prevede che *"il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

La centralità della formazione nel GDPR

- ✓ l'art. 38, paragrafo 2, prevede che *"il titolare e il responsabile del trattamento, sostengono il DPO nell'esecuzione dei compiti di cui all'art. 39, fornedogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".*

- ✓ l'art. 39, paragrafo 1 lett. b), prevede che il DPO debba *"sorvegliare l'osservanza del presente regolamento …. nonché delle politiche del titolare e 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 attività di controllo;*

ISO/IEC 27001:2013 - la formazione come misura di sicurezza

A.7.2.2 - Consapevolezza della sicurezza delle informazioni, educazione e formazione

“L’organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento, siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero, inoltre, essere adeguatamente formati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati personali attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica”

Come adempiere all'obbligo di formazione

Tenuto conto della complessità della struttura organizzativa, della natura dei dati trattati, delle finalità perseguite e delle modalità con le quali vengono effettuate le attività di trattamento dei dati personali è necessario:

- prevedere, in sede di approvazione del bilancio, il budget per la formazione dei soggetti autorizzati (se presente anche del DPO),
- progettare adeguati programmi di formazione per ognuna delle classi omogenee degli autorizzati e definire i relativi piani di realizzazione;
- prevedere prove finali del percorso formativo;
- prevedere sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;

obbligo di dimostrare (accountability)

I contenuti del programma di formazione

Aspetti generali

- definizione di dato personale e di trattamento
- principi generali in materia di trattamento di dati personali
- basi giuridiche che legittimano il trattamento
- i soggetti del trattamento
- i diritti dell'interessato
- gli obblighi di compliance in materia di protezione dei dati personali con particolare riferimento alla sicurezza dei dati e dei sistemi
- Responsabilità e sistema sanzionatorio

Aspetti specifici

Oltre alla formazione sugli aspetti generali in materia di protezione dei dati personali è necessario attuare anche percorsi formativi, per classi omogenee di soggetti autorizzati, finalizzati a far conoscere le norme e le regole che caratterizzano ogni specifico ambito del trattamento (esempio: gestione risorse umane, marketing e profilazione, ambito sanitario ecc.)

La mancata erogazione della formazione ai soggetti autorizzati è sanzionabile?

l’art. 83, paragrafo 4 lett. a) del GDPR prevede una sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2 % del fatturato mondiale annuo dell’anno precedente, se superiore, nei casi in cui il titolare e il responsabile violino, tra gli altri, gli articoli da 25 a 39;

CONCLUSIONI

GDPR guide*

FT graphic/Dreamstime

* General Data Protection Regulation

Grazie per l'attenzione

Avv. Andrea Lisi
andrealisi@studiolegalelisi.it
andrea.lisi@legalmail.it
www.studiolegalelisi.it
www.anorc.eu