Il nuovo Regolamento europeo sulla protezione dei dati personali n. 679/2016: obblighi e adempimenti per le PP.AA

Franco Cardin – Lendinara 26.01.2018

Uno sguardo alla realtà digitale che stiamo vivendo dal punto di vista della digitalizzazione e della protezione dei dati personali

- Hai Facebook ?
- No
- Whatsapp ?
- No
- Instagram ?
- No
- Telegram ?
- No niente, però se vuoi sono proprio qui di fronte a te

@Ty_il_nano


A
Normal (Bias
EQ-120)
Noise
Reduction
IN
OUT
D-C60
TDK


www.shutterstock.com · 110799905

Spotify


Caviatore Giacomo-
2ª Legione Libica M.V.S.N.
1ª Coorte
Cirenaica
Bengasi
CATANIA
13-14
21-IX
1928
DISTRIBUZIONE
www.delcampe.net


WhatsApp

Dove sono i video che vediamo?


VICMODEM
ATARI
830
ACOUSTIC MODEM
ATARI

La digitalizzazione è un processo inevitabile che sempre di più permea ogni ambito della nostra vita e la normativa, sia europea che nazionale, ormai abbraccia in modo sempre più convinto il principio del «digital first». In questo nuovo contesto i nostri dati personali sono trattati in modo diffuso e spesso a nostra insaputa……..

La privacy nel XXI° secolo

Ma in questa nuova realtà i nostri dati sono sicuri?

Cybercrime: in Italia il fenon | The War - Il Pianeta delle Sc

https://www.franzrusso.it/security-privacy/cybercrime-italia-fenomeno-reati-informatici-cresciuto

50% | Cerca

InTime
Condivido per Comunicare

News | Social Media | E-commerce | Events&WebMarketing | Web&Tech | Mobile Tech | Startup Business

Cybercrime: in Italia il fenomeno dei reati informatici è cresciuto del 51% in 5 anni

Franz Russo | 5 luglio 2017 | Security & Privacy | Lascia un commento

201 CONDIVISIONI

In 5 anni il fenomeno del Cybercrime, reati informatici, in Italia è cresciuto del 51%. E' quanto emerge da un'analisi condotta da DAS. In rapporto alla popolazione, il fenomeno è più diffuso in Liguria mentre la Puglia è la regione con la più bassa densità di reati di questo tipo.

Una ricerca condotta da DAS, compagnia di Generali Italia specializzata nella tutela legale, evidenzia come il fenomeno del Cybercrime, i reati informatici, sia cresciuto in Italia, in 5 anni (dal 2010 al 2015), del 51%. La ricerca permette anche di conoscere quanto il fenomeno abbia colpito le nostre regioni. E quindi, la Liguria, con una denuncia all'autorità giudiziaria (per "truffe e frodi informatiche" e delitti "informatici") ogni 246 abitanti, è la regione italiana con la più elevata frequenza di reati informatici, seguita da Molise (con 1 denuncia ogni 290 residenti) e Valle d'Aosta (1/294).

Trovaci su Facebook

Scrivi qui per eseguire la ricerca

00:10
08/07/2017

ESCLUSIVO

I ministeri italiani sotto attacco degli hacker

Oltre agli Esteri anche la Difesa e la rappresentanza italiana alla Ue: la cyber intrusione si è protratta almeno per tutto il 2016. Tutta la rete, ambasciate comprese, è stata bucata. Una feroce offensiva dal danno incalcolabile. Che le autorità hanno preferito nascondere. E che ora l'Espresso vi rivela

DI FLORIANA BULFON

13 febbraio 2017

Le intrusioni di hacker al ministero degli Esteri, ma anche alla Rappresentanza italiana a Bruxelles e alla Difesa sono continue. La nostra

Assalto hacker all'Ateneo Pi

iltirreno.gelocal.it/pisa/cronaca/2017/09/21/news/assalto-hacker-all-ateneo-pisano-1.15885137

Assalto hacker all'Ateneo Pisano

L'attore Gere parla di «energie negative dai cinesi» C'è una lettera ufficiale contro l'iniziativa dell'Ateneo

di Carlo Venturini

21 settembre 2017

https://www.google.com/url?ct=abg&q=https://www.google.com/adsense/support/bin/request.py?contact=abg_afc...vpET62QrgBAGgBi6AB6DkiGmoB6a-G9gHANIIBwiAYRABGAGxCZvBLTzk7-rC2BMM&usg=AFQjCNEpxJrqy8hcFu-elRXDIwkMN-hVCw

Scrivi qui per eseguire la ricerca

00:13 25/09/2017

Ascol... | Provvedi... | : Unito, U... | Crescono... | Albo Collabor... | Rassegna Sta... | CON... | Corso: Pr... | (7) TRAS... | D.Lgs. 07... | Elena Bus... | I migliori ...

www.ilmessaggero.it/marche/web_ascoli_soto_comune-1205449.html

Cerca

ROMA | VITERBO | RIETI | LATINA | FROSINONE | ABRUZZO | MARCHE | UMBRIA | VIDEO | FOTO | NEXT | OROSCOPO | METEO

Ascoli, sito web del Comune violato da hacker siriani

DI RENATO PIERANTOZZI E' stato da poco ripristinato il sito web del Comune violato stamane da un hacker che ha pubblicato in home page un messaggio contro le repressioni del regime siriano. Si è trattato di un appello "al mondo" per far conoscere quello che sta avvenendo nel Paese mediorientale. L'attacco al sito è stato segnalato al Comune dalla polizia postale. I tecnici del Comune hanno provveduto ad oscurare tutto il sito web e per poi ripristinarlo intorno all'ora di pranzo. "Non sono stati violati dati o documenti", assicura il sindaco Guido Castelli in una nota.

Sabato 22 Agosto 2015, 14:29 - Ultimo aggiornamento: 14:41

In attesa di n01d05.cumulus-cloud.com...

16:59
28/01/2016

17/11/2015 17:48

CRIMINI INFORMATICI

Attacco hacker al server del Comune di Fiumicino

Cancellati tutti i dati del servizio sociale. Il sindaco Montino: "Ci saranno ripercussioni gravi"

Un attacco hacker al server del servizio sociale del Comune di Fiumicino ha cancellato tutti i dati. Dai rilievi dell'ufficio informatico del Comune è stato riscontrato un virus informatico che ha determinato la criptazione di tutti i file e database presenti sul server dedicato con il conseguente danneggiamento della banca dati e degli archivi informatici dei servizi sociali. Il dirigente dell'area avvocatura e affari generali ha presentato, in nome e per conto del Comune una denuncia contro ignoti. "È un danno enorme per noi - ha commentato il sindaco Esterino Montino - ed è per questo che, accanto all'indagine interna, è stata sporta denuncia alle autorità preposte per fare luce su quanto accaduto e risalire ai responsabili. Ci sono e ci saranno ripercussioni gravi - ha aggiunto il primo cittadino - su atti amministrativi relativi all'erogazione dei contributi economici in favore degli utenti, nei servizi di assistenza per anziani, minori e disabili". "Il virus - ha continuato Montino - ha contagiato il sistema informatico del Comune di Fiumicino intaccando anche i dati sensibili degli utenti seguiti dall'area servizi sociali e rischia di ripercuotersi nell'esercizio del pubblico ufficio nei confronti di utenti fragili e più esposti. Il Comune - ha concluso il sindaco - si è già riservato il diritto di costituirsi parte civile".

Redazione online

Altri articoli che parlano di...

Categorie (1)

Roma Capitale

http://laprovinciapavese.gelocal.it/pavia/cronaca/201! Attacco hacker al Comune, ...

File Modifica Visualizza Preferiti Strumenti ?

BELGIOIOSO

Attacco hacker al Comune, persi migliaia di dati

Un virus manda in tilt il server, si salvano solo anagrafe e tributi. Per ripristinare la rete sono stati chiamati gli esperti del Politecnico di Milano

HACKER ATTACCO MUNICIPIO

24 aprile 2015

www.ilgiornale.it/news/cronache/hacker-attaccano-sito-tribunale-milano-e-quello-886589.html

Condividi:

Commenti: 15

Hacker attaccano il sito del Tribunale di Milano e quello dell'amministrazione carceraria

Sull'homepage compare un messaggio e la maschera di V per Vendetta (usato da Anonymous). Sotto attacco anche il sito del Dipartimento amministrazione penitenziaria

Raffaello Binelli - Sab, 16/02/2013 - 16:25

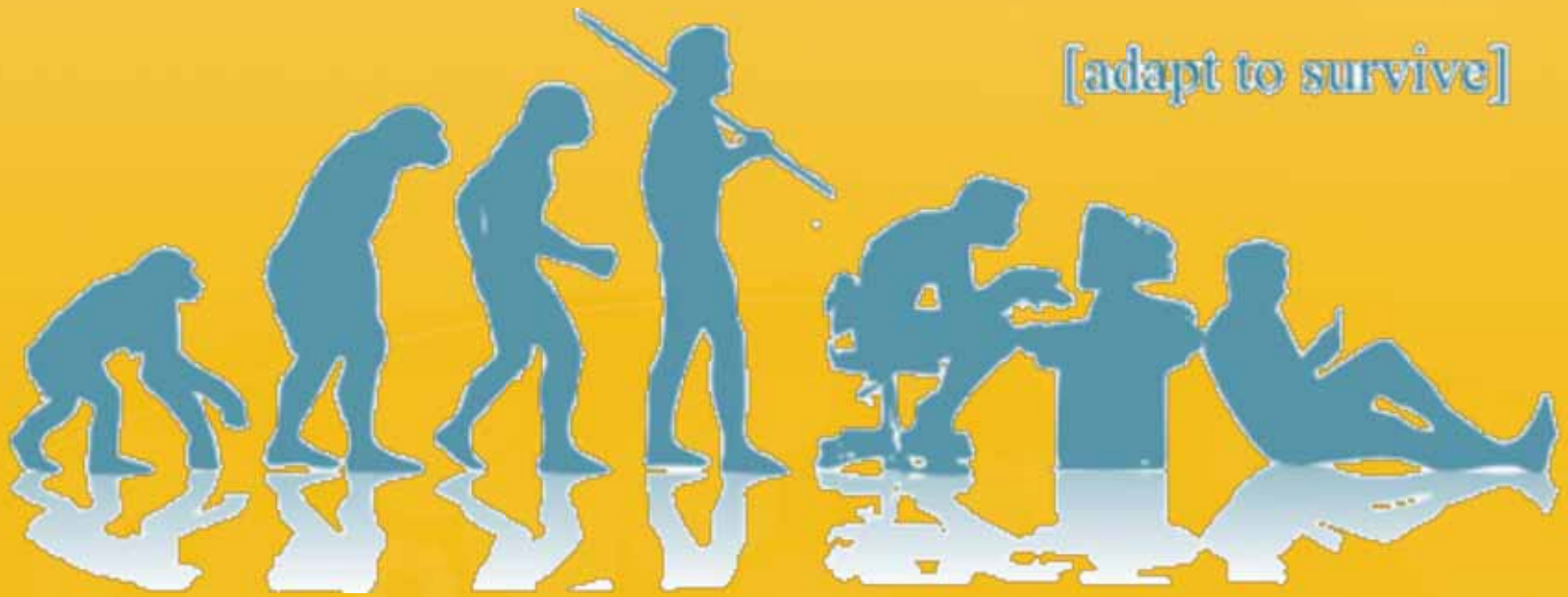
Doppio attacco hacker: uno contro il Dap (Dipartimento amministrazione penitenziaria), l'altro contro il sito del Tribunale di Milano.

La pagina internet del dipartimento che gestisce le carceri in Italia è irraggiungibile

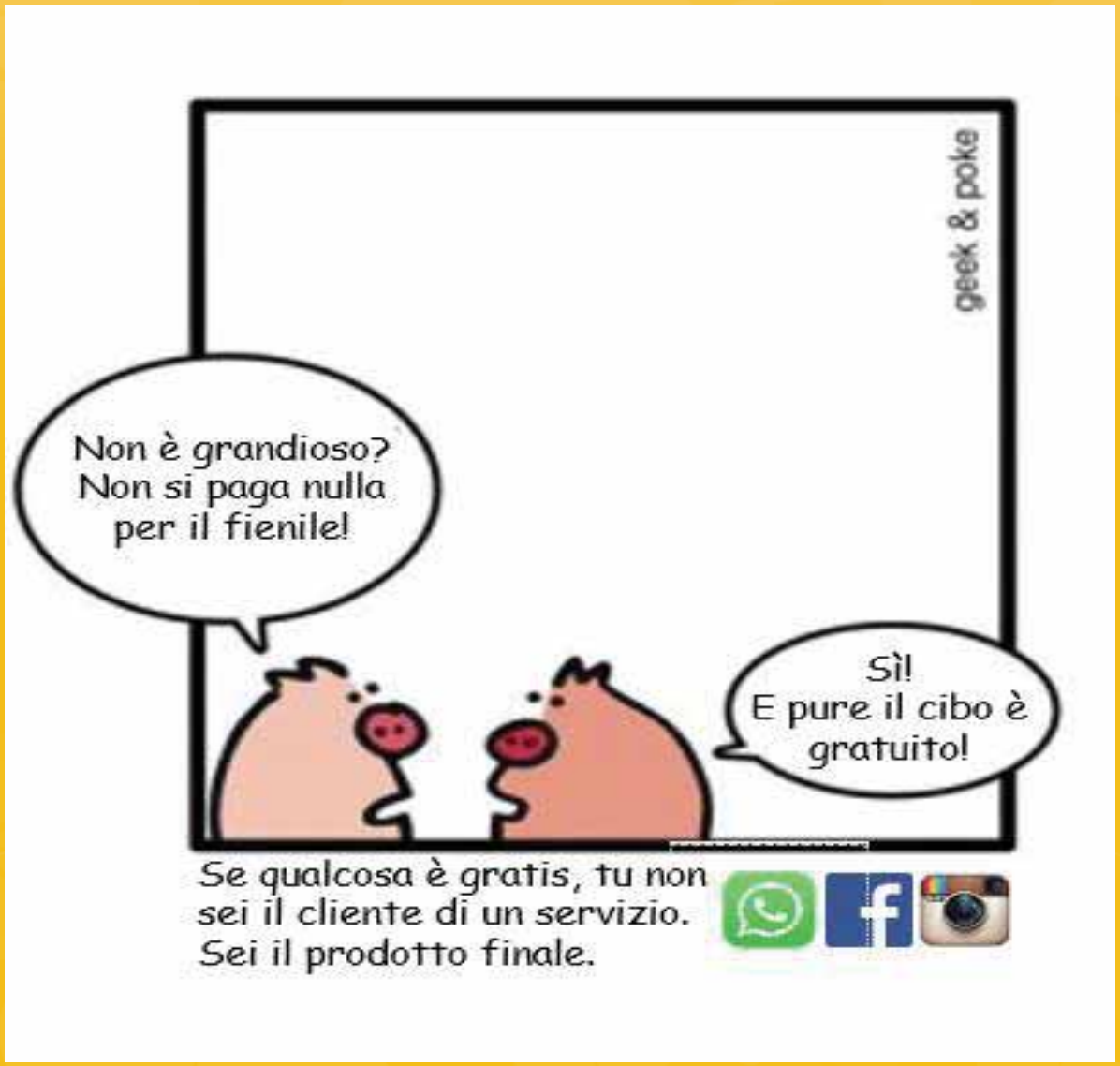
Editoriali

Italiani in arresto
di Alessandro Sallusti

...ormai ci siamo evoluti (o involuti?) in un nuovo modello di convivenza sociale e viviamo on line la nostra esistenza, dove i dati sono sempre di più una «merce di scambio»...



Il valore delle informazioni



Il percorso di approvazione del nuovo Regolamento (UE) 679/2016

composto da 173 considerando e da 99 articoli.

Perché questo nuovo regolamento?

- L’aumento sempre più significativo della raccolta e della condivisione di informazioni riguardanti le persone fisiche - dovuto alla rapidità dell'evoluzione tecnologica e alla globalizzazione - comportano nuove sfide per la protezione dei dati personali.

- Questa evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell’UE, affiancato da efficaci misure di attuazione, in grado di creare il clima di fiducia che consenta lo sviluppo dell’economia digitale in tutto il mercato interno UE.

Perché questo nuovo regolamento?

- È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

- Sebbene i suoi principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'UE, né ha eliminato la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche.

Previsione di un margine di flessibilità lasciato agli Stati membri per alcune tipologie di trattamento

- **Considerando 8** - Ove il presente regolamento prevede specificazioni o limitazioni (cfr. art. 23) delle sue norme ad opera del diritto degli Stati membri, gli stessi possono integrare elementi del presente regolamento nel proprio diritto nazionale;

- Il rinvio espresso al legislatore nazionale è previsto per i trattamenti effettuati nell'ambito:
  - sanitario **(cfr. art. 9.4)**
  - delle attività di giornalismo o di espressione accademica, artistica e letteraria **(cfr. art. 85)**;
  - del diritto di accesso ai documenti amministrativi e degli obblighi di trasparenza delle PP.AA **(cfr. art. 86)**;
  - dell'attribuzione e utilizzo di un numero di identificazione nazionale **(cfr. art. 87)**;
  - della gestione dei rapporti di lavoro **(cfr. art. 88)**;
  - degli obblighi di archiviazione nel pubblico interesse e delle attività di ricerca scientifica, statistica e storica **(cfr. art. 89)**;

- Il Regolamento fa rinvio al legislatore nazionale anche rispetto alla possibilità di prevedere eventuali sanzioni penali.

Adeguamento del quadro normativo nazionale al GDPR

- **Art. 13 legge 25.10.2017, n. 163** - Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679;
- **Art. 28 legge 20.11.2017, n. 167** – Modifica dell'art. 29 del D.Lgs. 196/03 e introduzione del nuovo art. 110-bis "Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici;
- **Art. 1, commi da 1020 a 1025, della legge 27.12.2017** "Bilancio di previsione dello Stato per l'anno finanziario 2018".

Aspetti invariati o variati marginalmente

- Definizione di dato personale (identificativo on line, geolocalizzazione)
- Definizione di trattamento
- Principi generali per il trattamento di dati personali
- Condizioni di liceità del trattamento (legittimo interesse del titolare)
- Obbligo di fornire l'informativa (forma e maggiori contenuti)
- Obbligo di acquisire, quando necessario, il consenso
- Soggetti che effettuano il trattamento (rappresentante del titolare e del responsabile del trattamento, sub-responsabile)

Principali novità

- Introduzione del principio di responsabilizzazione (accountability)
- Approccio basato sulla “Privacy by design” e “Privacy by default”
- Adozione di misure tecniche ed organizzative adeguate
- Valutazione d’impatto sulla protezione dei dati
- Obbligo di tenere il registro delle attività di trattamento
- Designazione Responsabile della protezione dei dati personali (Data Protection Officer – DPO)
- Notifica e comunicazione degli eventi di “data breach”
- Responsabilità civile solidale tra titolare, contitolare e responsabile del trattamento
- Nuovo sistema sanzionatorio

Principio di responsabilizzazione (accountability)

Art. 5.1 - I dati personali sono:

- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati;
- esatti e, se necessario, aggiornati;
- conservati per un tempo non superiore al conseguimento delle finalità per cui sono stati raccolti;
- trattati in modo da garantire un'adeguata sicurezza;

Art. 11 D.Lgs. 196/03

Art. 5.2 - "Il titolare del trattamento **è competente** per il rispetto dei suddetti principi **e in grado di comprovarlo** (responsabilizzazione).

Principio di responsabilizzazione (accountability)

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.

Principio di responsabilizzazione (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.

WP29 – Parere 3/2010 sul principio di accountability

Modalità e termini con i quali deve essere fornita l'informativa (art. 12)

- normalmente va resa per iscritto, anche con mezzi elettronici, oppure oralmente se richiesto dall'interessato di cui sia comprovata l'identità;
- deve essere facilmente accessibile, trasparente, concisa, semplice e chiara (nel caso sia rivolta a minori deve essere utilizzato un linguaggio a loro comprensibile;
- i contenuti dell'informativa possono essere resi anche mediante icone standardizzate leggibili da dispositivo automatico (atto delegato della Commissione);
- l'informativa ex art. 13 deve essere fornita nel momento della raccolta dei dati personali, mentre quella ex art. 14 va data al massimo entro un mese dall'ottenimento dei dati personali;

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (luglio 2017)

CONTENUTI DELL'INFORMATIVA

cosa cambia

I contenuti dell'informativa sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare:

- i dati di contatto del DPO ove esistente;
- la base giuridica del trattamento;
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali garanzie;
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo;
- il diritto di presentare un reclamo all'autorità di controllo;
- se il trattamento comporta processi decisionali automatizzati (compresa la profilazione) indicando la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (luglio 2017)

Raccomandazioni

- È opportuno che i titolari del trattamento verifichino la rispondenza delle informative attualmente utilizzate, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.

- Qualora i dati non siano stati raccolti presso gli interessati, spetta al titolare valutare lo sforzo sproporzionato richiesto per informarli. E' consigliato fare riferimento ai criteri evidenziati nei provvedimenti con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda doc.web 39624, doc.web 3864423 in tema di esonero dagli obblighi di informativa).

Responsabile del trattamento (art. 28)

- deve essere individuato sulla base dell'esperienza, della capacità e dell'affidabilità e, quindi, deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

- I trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile al titolare del trattamento e che regoli l'oggetto e la durata del trattamento, la finalità perseguita, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

- Il responsabile può ricorre a un altro responsabile solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Attenzione

- La corretta contrattualizzazione dei rapporti tra i diversi soggetti (titolari/contitolari/responsabili/sub-responsabili) che concorrono a vario titolo nella gestione delle attività di trattamento assume un'importanza significativa (si pensi, ad esempio, al caso dei servizi in cloud);

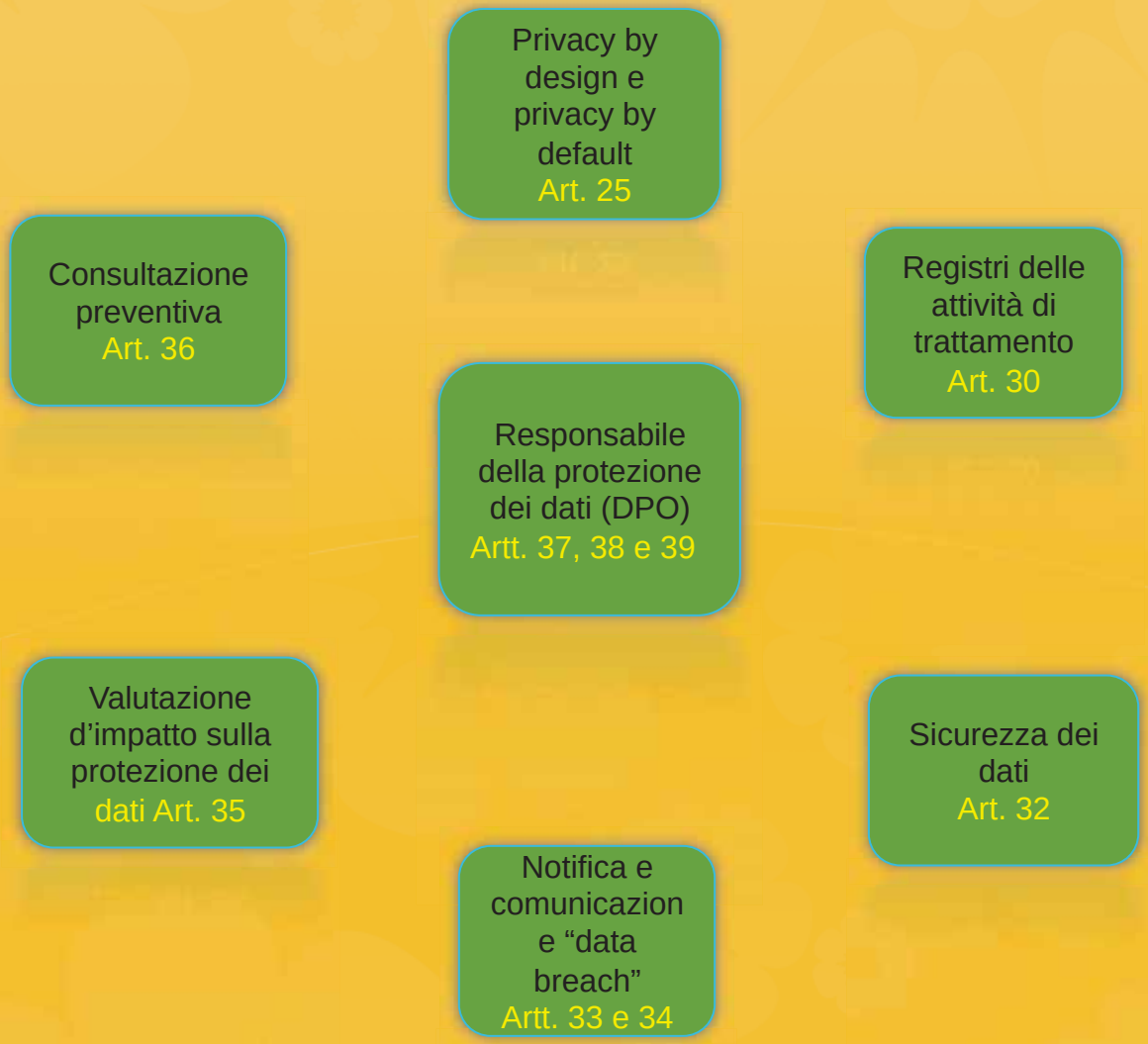
- La mancata o inadeguata contrattualizzazione, con particolare riferimento all'adozione delle specifiche misure di sicurezza, possono implicare una responsabilità solidale (cfr. art. 82, paragrafi 4 e 5).

Trattamento sotto l'autorità del titolare o del responsabile del trattamento (art. 29)

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento (gli attuali incaricati) che abbia accesso a dati personali non può trattare 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.

è consigliabile continuare ad applicare quanto previsto dall'attuale art. 30 del D.Lgs. 196/03

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



Il responsabile della protezione dei dati (DPO) (art. 37 - designazione)

La designazione del DPO da parte del titolare e del responsabile **è obbligatoria** quando il trattamento:

- è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;
- consiste in attività di monitoraggio regolare e sistematico su larga scala;
- riguarda dati sensibili e giudiziari su larga scala;

Il diritto dell'Unione o degli Stati membri possono prevedere altri casi per i quali è obbligatorio designare un DPO

Il responsabile della protezione dei dati (DPO) (art. 37 - designazione)

Nei seguenti casi è possibile designare un unico DPO

Gruppo di imprese (paragrafo 2)	a condizione che sia facilmente raggiungibile da tutte le sedi operative delle imprese
Più autorità pubbliche o organismi pubblici (paragrafo 3)	tenuto conto della struttura organizzativa e della dimensione (es. piccoli comuni)
Associazioni di categoria (paragrafo 4)	può agire per dette associazioni e altri organismi rappresentanti i titolari o i responsabili del trattamento

Il responsabile della protezione dei dati (DPO) (art. 37 – designazione)

- è designato in funzione della conoscenza specialistica della normativa in materia di protezione dei dati personali e della qualificata esperienza sull'applicazione della stessa;

- può essere un dipendente del titolare o del responsabile del trattamento oppure un professionista o una società sulla base di un contratto di servizi (assenza conflitto di interessi);

- i dati di contatto del DPO devono essere resi pubblici e comunicati all'autorità di controllo.

Il responsabile della protezione dei dati (DPO) (art. 38 – posizione)

- deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- deve essere sostenuto nell'esecuzione dei suoi compiti con le necessarie risorse umane, tecnologiche e finanziarie;
- non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti;
- non può essere rimosso o penalizzato per l'adempimento dei propri compiti;
- riferisce direttamente al vertice gerarchico;
- funge da punto di contatto per gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

Il responsabile della protezione dei dati (DPO) (art. 39 – compiti)

Il responsabile della protezione dei dati è incaricato **almeno** dei seguenti compiti:

- informa e fornisce consulenza, anche ai dipendenti che eseguono il trattamento, in merito agli obblighi previsti in materia di protezione dei dati personali;
- sorveglia l'osservanza dei predetti obblighi e degli eventuali disciplinari interni, incluso il riparto delle responsabilità e la formazione del personale;
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati personali e ne sorveglia lo svolgimento ai sensi dell'art. 35;
- funge da punto di contatto per l'autorità di controllo e coopera con la medesima per tutte le questioni connesse al trattamento dei dati personali, inclusa la consultazione preventiva di cui all'art. 36.

Nell'eseguire i propri compiti il DPO deve valutare attentamente i rischi inerenti al trattamento posto in essere, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

Faq del Garante sul DPO in ambito pubblico

- Se il DPO è un dipendente quale qualifica deve avere?
  Fermo restando che non devono sussistere motivi di conflitto di interessi con le altre attività che ordinariamente il dipendente svolge, è preferibile, tenuto conto della complessità organizzativa, designare un dirigente o un funzionario di alta professionalità;

- Quali certificazioni sono idonee a legittimare il DPO nell'esercizio delle sue funzioni?
  Nessuna!! La valutazione dei requisiti necessari al DPO per svolgere i propri compiti spetta alle PP.AA.

- Come deve essere designato il DPO?
  Se dipendente con apposito atto formale. Se esterno, la designazione deve costituire parte integrante del contratto di servizi (cfr. schema allegato alle faq). Nell'atto di designazione devono risultare le motivazioni della scelta del DPO (accountability).

Faq del Garante sul DPO in ambito pubblico

- La designazione di un DPO interno richiede necessariamente anche la costituzione di un apposito ufficio?
  Più aumentano complessità (sia organizzativa che tecnologica) e/o sensibilità dei trattamenti effettuati, tanto maggiori dovrebbero essere le risorse messe a disposizione del DPO.

- E' ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un DPO?
  No! è possibile l'individuazione di figure di supporto al DPO con riferimento a settori o ambiti territoriali diversi.

- Possono essere assegnati al DPO ulteriori compiti e funzioni?
  Si, a condizione che non comportino conflitto di interessi (definizione delle finalità e modalità dei trattamenti) e che non creino un cumulo di impegni tali da incidere negativamente sull'effettività dei compiti che il DPO deve svolgere ex art. 39.

Privacy “by design” e privacy “by default” (art. 25)

- Le **applicazioni** e i **servizi** che comportano il trattamento di dati personali devono tener conto, fin dalla loro progettazione dei principi e delle regole previste dal Regolamento in modo da minimizzare a priori non solo la raccolta dei dati, ma anche le operazioni di trattamento successive (cfr. considerando 78)

- Utilizzo di tecniche, quali ad esempio la minimizzazione e la pseudonimizzazione, che consentano di garantire che vengano trattati solo i dati personali strettamente necessari alle finalità perseguite, secondo i principi di necessità, pertinenza adeguatezza e non eccedenza (cfr. art. 3 D.Lgs. 196/03)

Considerando 78

.....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 dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati 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.

Registri delle attività di trattamento (art. 30)

- Il titolare e il responsabile del trattamento devono tenere, in forma scritta, anche in formato elettronico, un registro delle attività di trattamento svolte sotto la propria responsabilità i cui contenuti sono elencati rispettivamente nei paragrafi 1 e 2 dell'art. 30;

- Questo obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa rappresentare un rischio per i diritti e le libertà degli interessati, non sia occasionale o includa il trattamento di dati sensibili o giudiziari;

- In caso di eventuali ispezioni il registro delle attività di trattamento deve essere messo a disposizione dell'autorità di controllo;

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (luglio 2017)

- La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari e i responsabili del trattamento, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

- Niente vieta a un titolare o responsabile di inserire - oltre a quelle previste dall'art. 30 del GDPR - ulteriori informazioni proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Come costruirlo

- Gestione centralizzata del registro assicurando però il coinvolgimento costante nella procedura di redazione - ma soprattutto di aggiornamento - dei soggetti che hanno una più ampia visione delle attività di trattamento e che devono essere responsabilizzati e formati in ordine al valore aggiunto che tale documento può apportare al fine di assicurare una gestione corretta e trasparente dei flussi di dati personali;

- Il Registro è prima di tutto uno strumento per mappare i flussi dei trattamenti di dati all'interno dell'organizzazione e, quindi, è opportuno aggiungere ulteriori informazioni inerenti ai database che contengono le informazioni trattate, i software mediante i quali i dati vengono processati e i server utilizzati nei trattamenti.

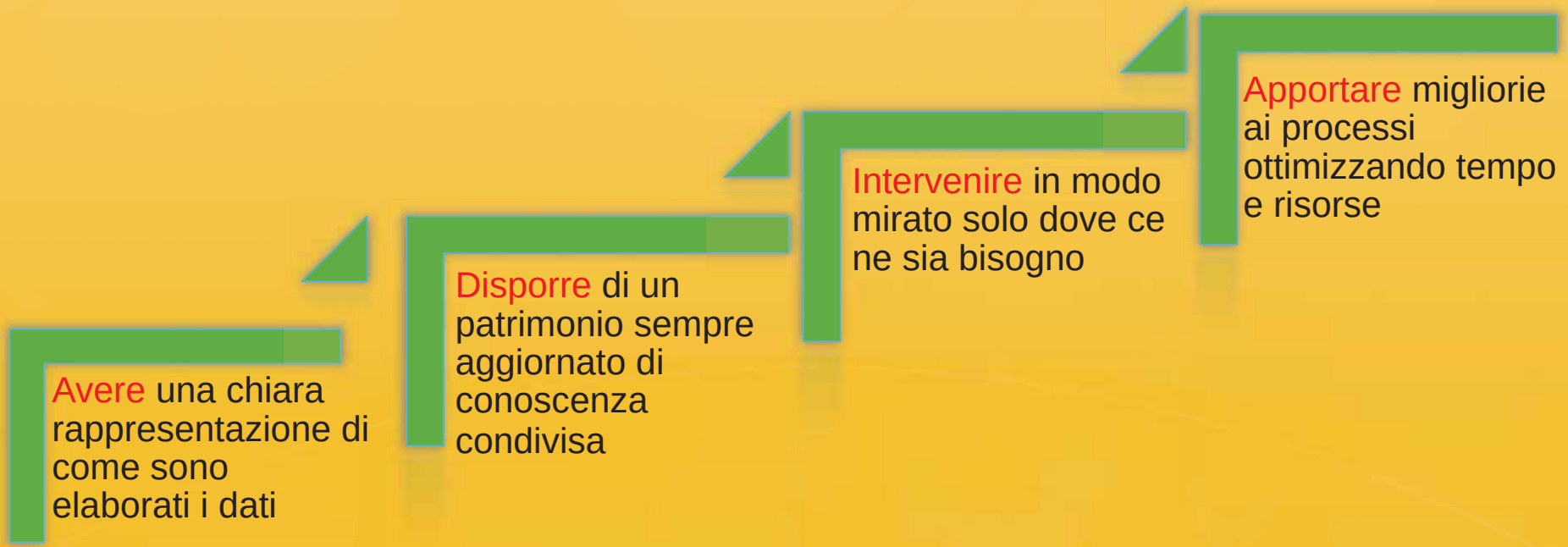
Aggiornamento del registro delle attività di trattamento

- 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!!!!

Il registro delle attività di trattamento può essere utilizzato per...

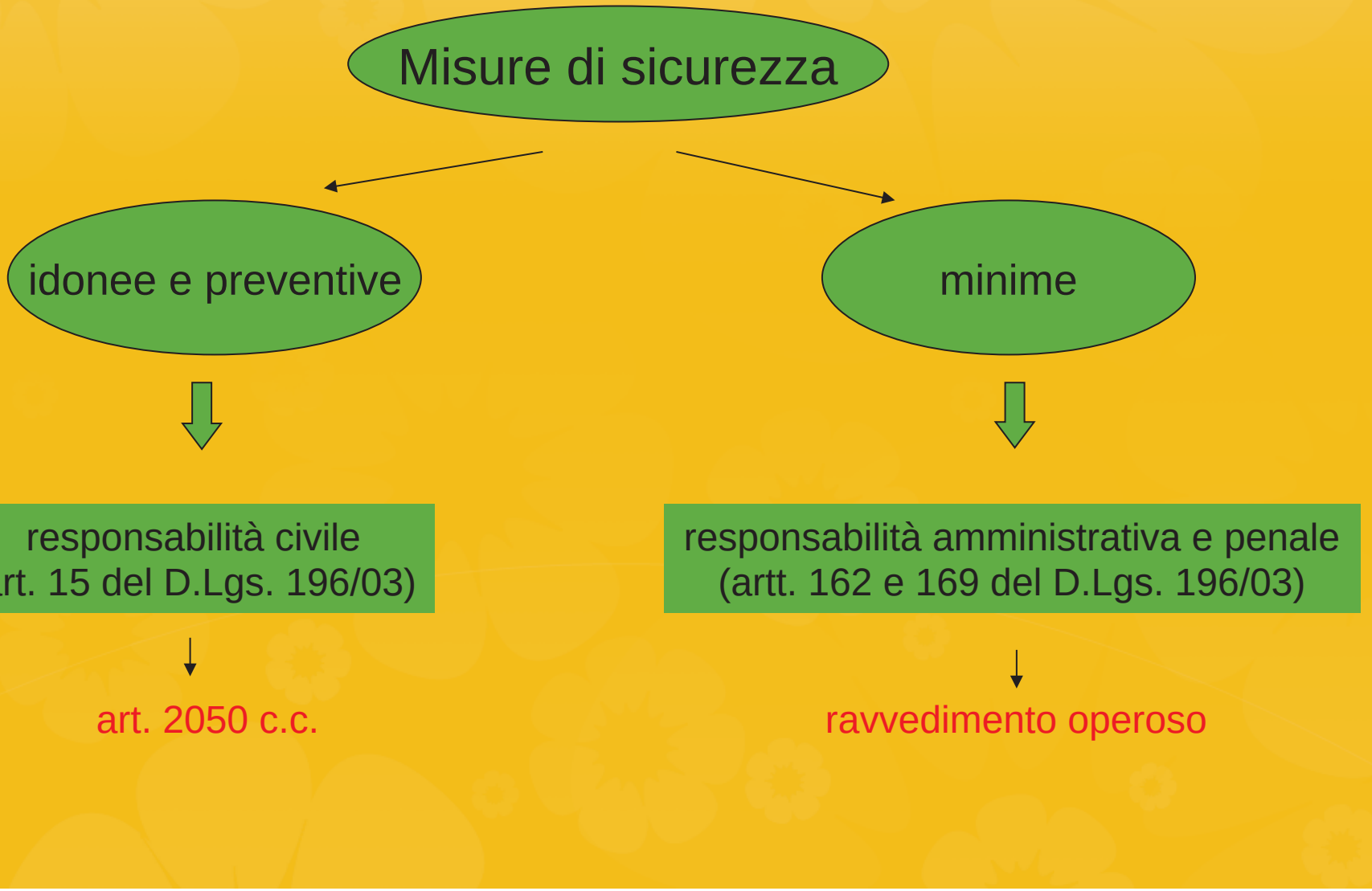


Le misure di sicurezza confronto tra D.Lgs. 196/03 e GDPR

Le misure di sicurezza nel D.Lgs. 196/03

- Misure idonee e preventive (art. 31)
- Misure minime (artt. 33, 34 e 35 – Disciplinare tecnico allegato B)
- Misure “necessarie” 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 e responsabilità nel D.lgs. 196/03



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: "... 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"

Notifica e comunicazione delle violazioni dei dati personali (data breach)

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

- Provvedimento del Garante **n. 161 del 4 aprile 2013 -** obbligo, per i fornitori di servizi telefonici e di accesso a internet, di comunicare la violazione dei dati personali subita entro 24 ore dalla conoscenza della violazione, fornendo gli eventuali elementi ulteriori entro 3 giorni dalla stessa;

- Provvedimento del Garante **n. 513 del 12 novembre 2014** - obbligo per i titolari (aziende, amministrazioni pubbliche) di comunicare entro 24 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi;

- Provvedimento del Garante **n. 393 del 2 luglio 2015 -** le amministrazioni pubbliche sono tenute a comunicare entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

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

- **Provvedimento del Garante n. 331 del 4 giugno 2015 “Linee guida in materia di Dossier sanitario”** – i titolari del trattamento sono tenuti a comunicare entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o degli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario;

- **Art.23, comma 9, del DPCM 29.09.2015, n. 178 “Regolamento in materia di fascicolo sanitario elettronico”** – Nel caso in cui i dati trattati nell’ambito del FSE subiscano violazioni tali da comportare la perdita, la distruzione o la diffusione indebita di dati personali, il titolare del trattamento effettua una segnalazione all’Autorità Garante entro una settimana dal verificarsi dell’evento, contenente:

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.

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 cambia 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);

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

Valutazione d'impatto sulla protezione dei dati (art. 35)

- Prima di iniziare un trattamento con l'utilizzo di nuove tecnologie informatiche o telematiche, che può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della natura dei dati personali trattati, del contesto in cui avviene il trattamento e delle finalità perseguite, il titolare deve effettuare una valutazione d'impatto sulla protezione di tali dati personali;

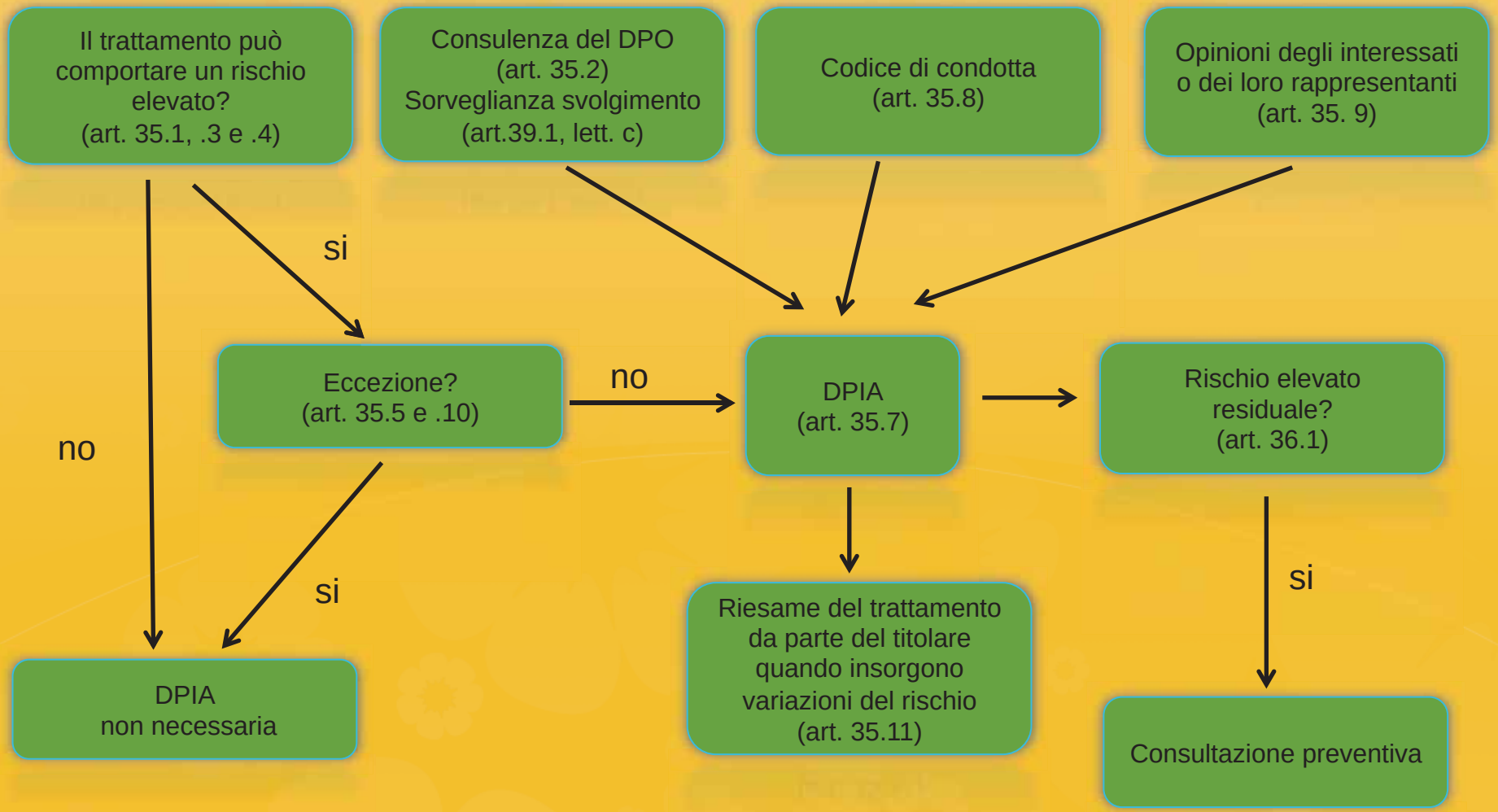
- La valutazione deve essere effettuata in particolare nei casi di:
  - attività sistematica di profilazione;
  - trattamento su larga scala di dati sensibili e giudiziari (es. ambito sanitario)
  - sorveglianza sistematica e su larga scala di una zona accessibile al pubblico (es. centri commerciali)

L'autorità di controllo redige e rende pubblici gli elenchi delle tipologie di trattamenti per i quali è dovuta o meno la valutazione d'impatto sulla protezione dei dati personali;

Consultazione preventiva (art. 36)

Qualora la valutazione d'impatto sulla protezione dei dati personali effettuata, indichi che il trattamento presenta un rischio elevato e le misure per attenuarlo siano impraticabili dal punto di vista della tecnologia disponibile e per gli elevati costi di attuazione, Il titolare deve consultare preventivamente l'autorità di controllo la quale nell'ambito dei suoi compiti di consulenza fornisce entro un termine di 2 mesi un parere scritto

Valutazione d'impatto sulla protezione dei dati (DPIA) quando e come eseguirla?



Responsabilità civile e sistema sanzionatorio

Diritto al risarcimento e responsabilità (art. 82)

- Chiunque subisca un danno materiale o immateriale *(patrimoniale e non patrimoniale)* causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento;

- Un titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il regolamento.

- Un responsabile del trattamento risponde per il danno causato solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento;

Diritto al risarcimento e responsabilità (art. 82)

- Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile;

- Qualora più titolari del trattamento o responsabili del trattamento, oppure entrambi, siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato;

Importanza della corretta contrattualizzazione dei rapporti tra contitolari o tra titolari e responsabili

Diritto al risarcimento e responsabilità (art. 82)

- Il titolare o il responsabile del trattamento che ha risarcito l'intero danno, ha il diritto di rivalersi sugli altri titolari o responsabili, coinvolti nello stesso trattamento, della parte del risarcimento corrispondente alla loro parte di responsabilità per il medesimo danno;

- Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro.

Sistema sanzionatorio

- Considerando 11 - Un'efficace protezione dei dati personali in tutta l'Unione presuppone ..... sanzioni equivalenti per le violazioni negli Stati membri;

- Considerando 13 - Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca ..... e assicuri sanzioni equivalenti in tutti gli Stati membri;

Poteri delle Autorità di controllo (art. 58)

Poteri di indagine (art. 58.1)

controllare l'effettiva applicazione del regolamento;
accertare le possibili violazioni (si attivano sia sulla base di un ricorso da parte dell'interessato sia su iniziativa autonoma dell'autorità di controllo)

Poteri correttivi (art. 58.2)

ingiungere al titolare o al responsabile del trattamento di soddisfare una richiesta dell'interessato, di comunicargli la violazione dei dati, di limitare il trattamento o rettificare/cancellare i dati;
infliggere una sanzione amministrativa pecuniaria;

Poteri autorizzativi e consultivi (art. 58.3)

fornire consulenza al titolare del trattamento (consultazione preventiva);
rilasciare pareri al Parlamento o al Governo nazionale; autorizzare le clausole contrattuali ecc.

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83)

- Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte in relazione alle violazioni del regolamento siano in ogni singolo caso effettive, proporzionate e dissuasive;

- Le sanzioni amministrative pecuniarie sono inflitte in aggiunta o in luogo delle misure imposte dall'autorità di controllo nell'ambito dell'esercizio dei propri poteri correttivi;

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.4)

La violazione delle seguenti disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) obblighi del titolare del trattamento e del responsabile del trattamento
   - consenso dei minori (art. 8);
   - trattamento che non richiede l'identificazione (art. 11);
   - principi di privacy by design e by default (art. 25);
   - accordo interno per determinare responsabilità tra contitolari (art. 26);
   - nomina del rappresentante di titolari o dei responsabili non stabiliti nell'Unione e i suoi compiti (art. 27);
   - compiti e responsabilità del responsabile del trattamento (art. 28);
   - trattamento da parte dei dipendenti e collaboratori del titolare o del responsabile (art. 29);

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.4)

- tenuta dei registri delle attività di trattamento (art. 30);
- cooperazione del titolare o del responsabile del trattamento con l'autorità di controllo (art. 31);
- adozione di misure di sicurezza adeguate (art. 32);
- notifica all'autorità di controllo di una violazione di dati personali (art.33);
- comunicazione all'interessato di una violazione di dati personali (art. 34);
- valutazione d'impatto (art. 35);
- consultazione preventiva (art. 36);
- designazione del DPO (art. 37);
- obblighi del titolare e del responsabile nei confronti del DPO (art. 38);
- compiti assegnati al DPO (art. 39);
- obblighi in materia di certificazione (art. 42).

Condizioni generali per infliggere sanzioni amministrative pecuniarie (art. 83.5)

La violazione delle seguenti disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) principi generali applicabili al trattamento (art. 5), condizioni di liceità del trattamento (art. 6), condizioni per il consenso (art. 7) e trattamento di categorie particolari di dati personali (art. 9);
b) diritti degli interessati (artt. da 12 a 22);
c) trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
d) obblighi previsti dalle legislazioni degli Stati membri adottate a norma del capo IX (giornalismo, espressione accademica o letteraria, accesso ai documenti delle PA, rapporti di lavoro, archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica);
e) negato accesso all'autorità di controllo durante l'esercizio dei propri poteri di indagine o inosservanza di un suo provvedimento di carattere correttivo;

Documenti del Gruppo di lavoro ex art. 29, riguardanti l'applicazione del GDPR

- WP 242 "Linee guida sul diritto alla portabilità dei dati" (adottate il 13.12.2016, come modificate e adottate da ultimo il 5.4.2017)
- WP 243 "Linee guida sui responsabili della protezione dei dati personali" (adottate il 13.12.2016, come modificate e adottate da ultimo il 5.4.2017)
- WP 244 "Linee guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento" (adottate il 13.12.2016, come modificate e adottate da ultimo il 5.4.2017)
- WP 248 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato" (adottate il 4.4.2017, come modificate e adottate da ultimo il 4.10.2017)

Documenti del Gruppo di lavoro ex art. 29, riguardanti l'applicazione del GDPR

- WP 250 "Linee guida in materia di notifica delle violazioni di dati personali" (adottate il 3.10.2017, attualmente in consultazione pubblica)
- WP 251 "Linee guida in materia di processi decisionali automatizzati e profilazione" (adottate il 3.10.2017, attualmente in consultazione pubblica)
- WP 253 "Linee guida in materia di applicazione e definizione delle sanzioni amministrative" (adottate il 3.10.2017)

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
Valutazione dei rischi e definizione delle politiche di sicurezza

FASE - 6
Implementazione del processo di data breach

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