Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Nuovo regolamento privacy: come organizzarsi

a cura di Fabio Di Resta
9 maggio 2018



Situazione attuale in Italia prima del Regolamento EU

I soggetti coinvolti secondo il Codice della Privacy (d.lgs. 196/2003)

- **Titolare del trattamento dei dati personali**
  - Co-Titolare
- Responsabile del trattamento dei dati personali
- Incaricato del trattamento dei dati personali

Definizioni rilevanti Codice della Privacy

Titolare:
definizioni del T.U:

f) "*titolare*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Art. 28
Titolare del trattamento

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Il "TITOLARE" è l'azienda/ente nel complesso.

Conseguentemente nel caso concreto "TITOLARE" è: analisi della fattispecie

Potere decisionale autonomo in ordine alla finalità e alle modalità del trattamento

Situazione attuale in Italia prima del Regolamento EU

I soggetti coinvolti secondo il Codice della Privacy (d.lgs. 196/2003)

- Titolare del trattamento dei dati personali
  - **Co-Titolare**
- Responsabile del trattamento dei dati personali
- Incaricato del trattamento dei dati personali

Situazione attuale in Italia prima del Regolamento EU

Contitolarità (art. 26 del Regolamento generale)

Non viene disciplinato del Codice della Privacy

Viene disciplinato dalla prassi decisoria del Garante (*Parere Garante privacy del 30 giugno 1997*):

- Condivisione delle prerogative in ordine alle finalità e modalità del trattamento;
- Condivisione delle responsabilità del titolare del trattamento.

Situazione attuale in Italia prima del Regolamento EU

I soggetti coinvolti secondo il Codice della Privacy (d.lgs. 196/2003)

- Titolare del trattamento dei dati personali
  - Co-Titolare
- **Responsabile del trattamento dei dati personali**
- Incaricato del trattamento dei dati personali

Responsabile del trattamento: attenersi alle ISTRUZIONI IMPARTITE

Responsabile:
definizioni del Codice della Privacy:

g) "*responsabile*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Art. 29
Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. **I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.**

5. Il responsabile effettua il trattamento attenendosi alle ISTRUZIONI IMPARTITE DAL TITOLARE IL QUALE, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Per la legge non esiste differenza tra responsabile "interno" all'azienda (collegato da un rapporto di lavoro dipendente o assimilabile) ovvero "esterno" all'azienda/ente (collegato da un rapporto di lavoro NON dipendente).

Il "<u>responsabile</u>" è una <u>funzione</u>, ed infatti può essere anche un soggetto giuridico esterno alla struttura; tale soggetto è poi rappresentato pro-tempore da una determinata persona fisica.

Situazione attuale in Italia prima del Regolamento EU

I soggetti coinvolti secondo il Codice della Privacy (d.lgs. 196/2003)

- Titolare del trattamento dei dati personali
  - Co-Titolare
- Responsabile del trattamento dei dati personali
- **Incaricato del trattamento dei dati personali**

Incaricato ai sensi Codice della Privacy (d.lgs. 196/2003)

Incaricato:

h) "*incaricati*", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

Art. 30
Incaricati del trattamento

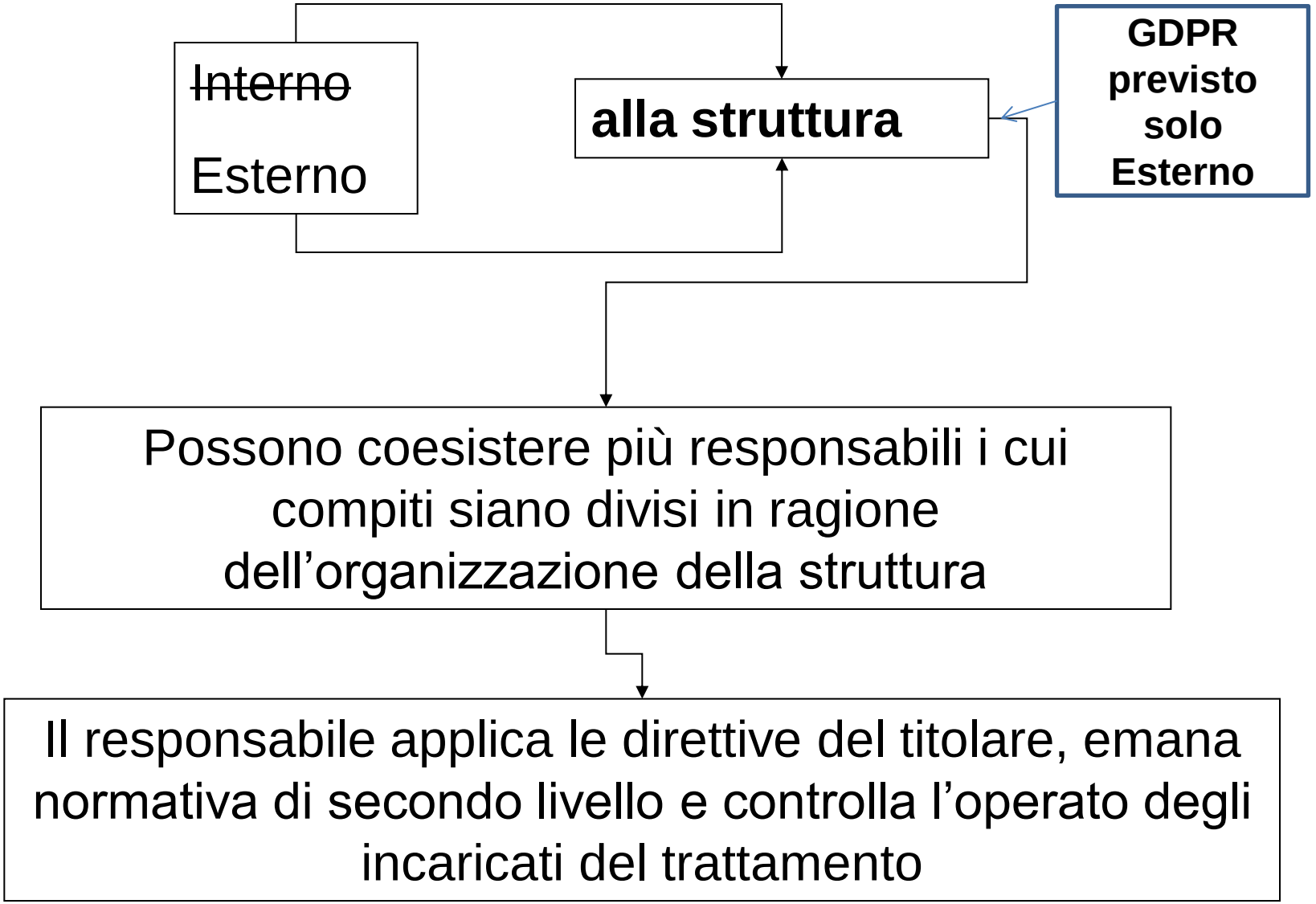
1. Le operazioni di trattamento possono essere effettuate solo da incaricati, che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Gli unici soggetti abilitati a "trattare" i dati sono gli "incaricati", pertanto anche il "titolare" e/o i "responsabili", quando materialmente trattano i dati, sono ANCHE "incaricati".

Sono "incaricati" del trattamento tutti i soggetti, a qualunque titolo, collaboratori e/o dipendenti delle varie articolazioni di un gruppo o un ente, come, per esempio, i collaboratori a progetto (ex co.co.co.), i dipendenti, gli "ex interinali" Ora somministrati), le persone fisiche che collaborino con fornitori di servizi, i consulenti, ecc.

Il Responsabile privacy - Codice della Privacy



Riflessione analitica sui compiti del responsabile privacy

Art. 29 del Codice della Privacy (legge 167/2017 sostiuito in vigore dal 12.12.17)

"5. Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie **istruzioni e di quanto stabilito negli atti di cui al comma 4-bis**."

Riflessione analitica sul responsabile privacy

Deve:

Attenersi alle istruzioni analitiche: compiti specifici conferiti dal

titolare e non definiti dalla legge

Limiti:

- Non può agire in modo indipendente ma seguire le istruzioni
- Non è prevista una disciplina che obbliga a fornire autonomia nella gestione delle risorse economiche, di personale, altro necessario per eseguire le proprie mansioni/o il proprio servizio
- Non è prevista alcuna disciplina in ordine al conflitto di interessi che si può presentare anche con altre funzioni affidate

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

Il ruolo di Supervisore Indipendente

Interno

(rapporto di lavoro subordinato – “assunto” o “membro del personale”)

Esterno

(contratto di servizi)

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

Il ruolo di Supervisore Indipendente

Interno

(rapporto di lavoro subordinato – “dipendente” art. 37 co. 6)

Esterno

(contratto di servizi)

DPO nel quadro normativo europeo e italiano protezione dei dati personali

Data Protection Officer (DPO)

Responsabile della protezione dei dati personali

L’incarico di DPO può essere affidato a persona giuridica oppure un ente assimilabile ad essa?

Articolo 37 Designazione del responsabile della protezione dei dati

Il responsabile del trattamento e l'incaricato del trattamento designano **sistematicamente** un responsabile della protezione dei dati quando:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala** (Si veda considerando n. 71)

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, **di categorie particolari di dati di cui all'art. 9 (dati sensibili inclusi i dati biometrici) o dati relativi alle condanne penali e a reati**

Esclusione dai trattamenti su larga scala: medico – operatore sanitario - avvocato

Articolo 37 Designazione del responsabile della protezione dei dati

Il responsabile del trattamento e l'incaricato del trattamento designano **sistematicamente** un responsabile della protezione dei dati quando:

- **Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (Si veda considerando n. 71)

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 (dati sensibili inclusi i dati biometrici) o dati relativi alle condanne penali e a reati

Esclusione dai trattamenti su larga scala: medico – operatore sanitario - avvocato

Articolo 37 Designazione del responsabile della protezione dei dati

Focus autorità pubblica e organismo pubblico

le linee guida pubblicate dal Gruppo indicano che le nozioni di “autorità pubblica ” e di “organismo pubblico” **devono riferirsi al diritto interno dello Stato Membro**. In tal senso vanno ricompresi i Ministeri e tutti gli enti pubblici anche territoriali, ma anche tutti gli enti gestiti secondo la normativa di diritto pubblico.

Articolo 37 Designazione del responsabile della protezione dei dati

Focus autorità pubblica e organismo pubblico

Infatti, come specificato dal Gruppo art. 29 alla nota 12 per gli organismi di diritto pubblico si può fare riferimento alla **direttiva 2003/98/UE** sul riutilizzo dell'informazione nel settore pubblico (come modificata dalla direttiva 2013/37/UE), al cui art. 2 punti numero 1 e 2 è previsto che:

"Ai fini della presente direttiva si intende per:

«ente pubblico», le autorità statali, regionali o locali, gli organismi di diritto pubblico e **le associazioni formate da una o più di tali autorità** oppure da uno o più di tali organismi di diritto pubblico;

2) «**organismo di diritto pubblico**», qualsiasi organismo:

a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale;

b) dotato di personalità giuridica;

c) la cui attività è finanziata **in modo maggioritario** dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui **gestione è soggetta al controllo di questi ultimi**, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito **da membri più della metà** dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico".

Articolo 37 Designazione del responsabile della protezione dei dati

Focus autorità pubblica e organismo pubblico d.lgs. 36/2006 di recepimento della Direttiva 2003/98/Ce

Art. 2.

Definizioni

1. Ai fini del presente decreto si intende per:

a) pubbliche amministrazioni: le amministrazioni dello Stato, le regioni, le province autonome di Trento e di Bolzano, gli enti pubblici territoriali e le loro unioni, consorzi o associazioni e gli altri enti pubblici non economici;

b) organismi di diritto pubblico: gli organismi, dotati di personalita' giuridica, istituiti per soddisfare specifiche finalita' d'interesse generale non aventi carattere industriale o commerciale, la cui attivita' e' **finanziata in modo maggioritario dallo Stato**, dalle regioni, dagli enti locali, da altri enti pubblici o organismi di diritto pubblico, o la cui **gestione e' sottoposta** al loro controllo o i cui organi d'amministrazione, di direzione o di vigilanza sono costituiti, **almeno per la meta', da componenti designati dai medesimi soggetti pubblici**. Sono escluse le imprese pubbliche, come definite all'articolo 2, comma 1, lettera b), del decreto legislativo 11 novembre 2003, n. 333;

Articolo 37 Designazione del responsabile della protezione dei dati

Il titolare del trattamento e il responsabile del trattamento designano **sistematicamente** un responsabile della protezione dei dati quando:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali

- **Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (Si veda considerando n. 71)**

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 (dati sensibili inclusi i dati biometrici) o dati relativi alle condanne penali e a reati

Esclusione dai trattamenti su larga scala: medico – operatore sanitario - avvocato

Articolo 37 Designazione del responsabile della protezione dei dati

Focus su attività principale

Con “attività principali” si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è **inscindibilmente connesso all’attività del titolare o del responsabile**. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

La gestione dell’attività per concorrenti finalità contabilità-amministrative rappresenta in genere da ritenersi accessoria, analoga considerazione vale anche per la gestione dell’infrastruttura informatica interna all’organizzazione

Articolo 37 Designazione del responsabile della protezione dei dati

Focus monitoraggio regolare e sistematico

«Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati*" ricomprendendovi senza dubbio tutte **le forme di tracciamento e profilazione su Internet** anche per finalità di **pubblicità comportamentale**.»

Articolo 37 Designazione del responsabile della protezione dei dati

Focus monitoraggio regolare e sistematico

«L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.»

Articolo 37 Designazione del responsabile della protezione dei dati

Focus monitoraggio regolare e sistematico

«L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del

WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia. »

Articolo 37 Designazione del responsabile della protezione dei dati

Focus monitoraggio regolare e sistematico
Tipologia di attività indicate dalle LG dell'Gruppo di lavoro ex art. 29

«Alcune esemplificazioni: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc. »

Focus sui compiti minimali del DPO
Supervisore indipendente (art. 37)

Informare e fornire consulenza al titolare o al responsabile del trattamento nonché i dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione europea o degli Stati membri relativi alla protezione dei dati personali

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

fornire, se richiesto, ***un parere*** in merito alla valutazione d'impatto sulla protezione dei dati e *sorvegliarne* lo svolgimento ai sensi dell'articolo 35;

cooperare con l'autorità di controllo e fungere da ***punto di contatto*** per l'autorità di controllo per questioni connesse al trattamento di dati personali.

Galassia delle attività del DPO



Elementi caratterizzanti l'indipendenza del DPO (art. 38)

Requisiti negativi

- assenza di un conflitto di interessi, *può svolgere altri compiti e funzioni*

- INDIPENDENZA: Non ingerenza nell'esercizio delle sue funzioni da parte del
- responsabile o incaricato: nessuna <<istruzione per quanto riguarda l'esecuzione dei propri compi>>
- <<non è rimosso o penalizzato[…] per l'adempimento dei propri compiti>>



concetto di indipendenza effettiva, nota a livello giurisprudenziale, in particolare, in ambito organizzativo come i Modelli di Organizzazione (c.d. MOGC secondo d.lgs. 231/2001) e i relativi Organismi di Vigilanza non solo monocratici

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Assenza del Conflitto di interessi e contesto legale-organizzativo dell'organizzazione

«A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare o del responsabile, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.»

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Assenza del Conflitto di interessi e contesto legale-organizzativo dell'organizzazione

Dubbi al DPO sono inibiti compiti operativi?

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Conflitto di interessi e contesto legale-organizzativo dell'organizzazione

Dubbi al DPO sono inibiti compiti operativi? IT manager e DPO

Bavarian DPA - BAY LDA 20 OTTOBRE 2016

Solo valido nel contesto BayLAD?



Responsabilità operativa rilevante

Autocontrollo

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Dubbi al DPO sono inibiti compiti operativi? IT Admintrator e DPO

Bavarian DPA - BAY LDA

Solo valido nel contesto BayLAD?



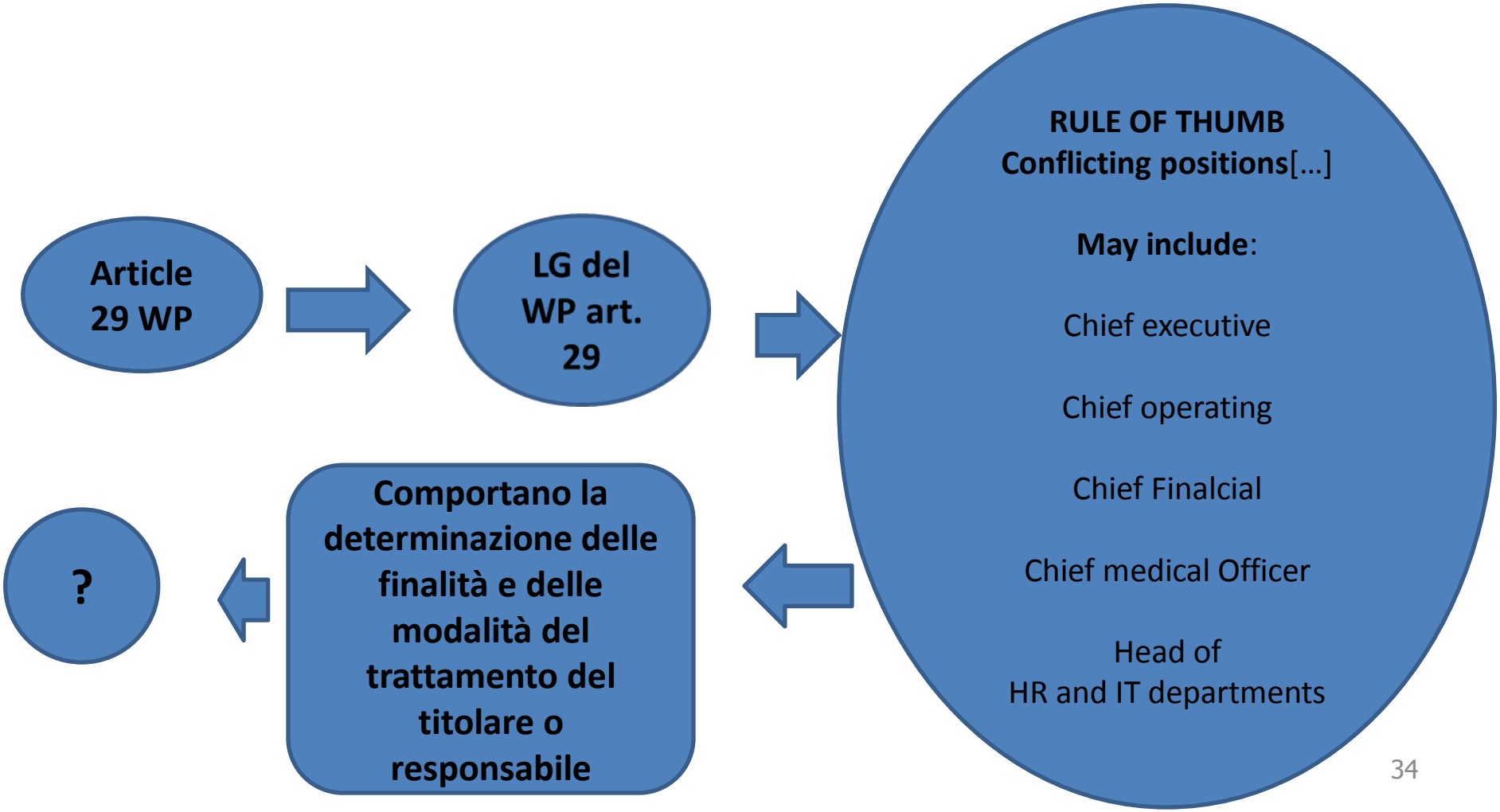
Responsabilità operativa rilevante

Autocontrollo

?

Elementi caratterizzanti l'indipendenza del DPO (art. 38 – Linee guida WP Art. 29)

Dubbi al DPO sono inibiti compiti operativi? IT Admintrator e DPO



Aspetti pratici sul DPO

Dopo questa analisi

Se mi affidano un compito come DPO cosa devo fare per prima cosa?

Consigliabile:

Fare una pre-assessment per valutare preliminarmente la complessità dell'organizzazione

Effettuare una gap analysis per capire la situazione attuale dell'organizzione rispetto ai requisiti del GDPR

Aspetti pratici sul DPO

Prima cosa da fare prima del conferimento dell'incarico di DPO.

Verificare che l'organizzazione abbia redatto un **codice etico o regole interne** a tale scopo onde evitare conflitti di interessi, altrimenti segnalare l'esigenza immediatamente

Aspetti pratici sul DPO

Prima cosa da fare è una riunione di insediamento del DPO.

Come primo step un DPO appena assunto l'incarico dovrà puntare a:

Redigere un completo Work Plan:

Definire gli obiettivi da raggiungere rispetto alla piena conformità

Definire le carenze a livello di politiche e procedure interne

Definire un piano delle attività di controllo periodiche

Definire un piani di informazione e sensibilizzazione

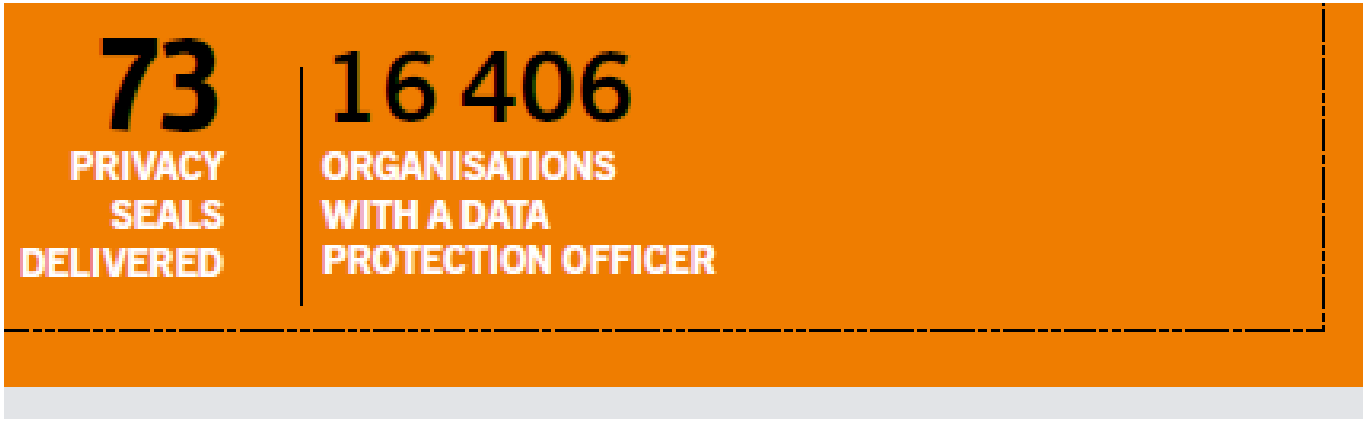
Definire un piano di formazione del personale

Definire un piano di revisione delle attribuzione dei ruoli e responsabilità ai fini privacy

Aspetti pratici sul DPO

L'opportunità del nuovo ruolo del DPO

Il Cnil – Autorità Garante privacy francese ha pubblicato un report riferito all'anno 2015 nel quale specifica che nonostante sia prevista nella normativa nazionale francese solo una designazione facoltativa vi erano fino al 2015 già
oltre 16.000 organizzazioni che avevano scelto di dotarsi di tale figura – nel 2017 hanno raggiunto le **18.000** organizzazioni



Link utili di approfondimento sul RPD/DPO

http://www.corrierecomunicazioni.it/it-world/29046_data-protection-officer-cosi-funzionera-in-italia.htm - **Data protection officer: così funzionerà in Italia – FABIO DI RESTA – 29 luglio 2014**

http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-09-26/dpo-data-protection-officer-responsabile-protezione-dati-personali-174216.php - **DPO – Data Protection Officer: il responsabile della protezione dei dati personali - CRISTIANO COMINOTTO – ANNA MINICHIELLO – FRANCESCO CURTARELLI – 20 giugno 2016**

http://www.agendadigitale.eu/infrastrutture/data-protection-officer-si-chiariscono-le-novita-del-regolamento-privacy-europeo_2844.htm - **Data protection officer, si chiariscono le novità del Regolamento privacy europeo – GABRIELE FAGGIOLI – 23 gennaio 2017**

http://www.corrierecomunicazioni.it/ict-law/45112_data-protection-officer-troppi-problemi-interpretativi-serve-piu-chiarezza.htm -

Data protection officer: troppi problemi interpretativi, fare chiarezza – FABIO DI RESTA – 27 dicembre 2016

http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2016-12-21/il-ruolo-data-protection-officer-anche-italia-e-obbligatorio-la-pubblica-amministrazione-e-ambito-privato-pubblicate-linee-guida-gruppo-europeo-garanti-privacy-121040.php **Il ruolo del Data Protection Officer anche in Italia è obbligatorio per la pubblica amministrazione e in ambito privato: pubblicate le linee guida del Gruppo europeo dei Garanti privacy – FABIO DI RESTA – 21 dicembre 2016**

http://www.agendadigitale.eu/infrastrutture/norme-privacy-ue-ecco-tutto-cio-che-bisogna-sapere-su-accountability-e-sicurezza_2279.htm - **Norme privacy UE, ecco tutto ciò che bisogna sapere su accountability e sicurezza – MAURO ALOVISIO E FABIO DI RESTA – 20 giugno 2016**

https://www.youtube.com/watch?v=sMpveaZKZ2A – **Compiti e responsabilità del "data protection officer - FABIO DI RESTA – 26 dicembre 2016**

https://www.agendadigitale.eu/sicurezza/gdpr-sanzioni-e-responsabilita-tutto-cio-che-ce-da-sapere/ - **Gdpr, sanzioni e responsabilità: tutto ciò che c'è da sapere – 3 gennaio 2018**

https://www.agendadigitale.eu/compiti-dpo **- Gdpr, la scelta del DPO: compiti e requisiti –17 gennaio 2018**

https://www.agendadigitale.eu/sicurezza/privacy/gdpr-scegliere-responsabile-trattamento-dati-ce-sapere/ **GDPR, scegliere il responsabile trattamento dati: interno o esterno all'azienda? - 28 febbraio 2018**

Nuove misure di prevenzione GDPR

Le violazione dei dati/data breach

Gli istituti di credito come le altre organizzazioni entro il 25 maggio 2017 devono essere in grado di gestire il data breach

ELIMINAZIONE O RIDUZION E SOSTANZIALE DEL PREGIUDIZIO CHE PUO' SUBIRE L'INTERESSATO

TRASPARENZA

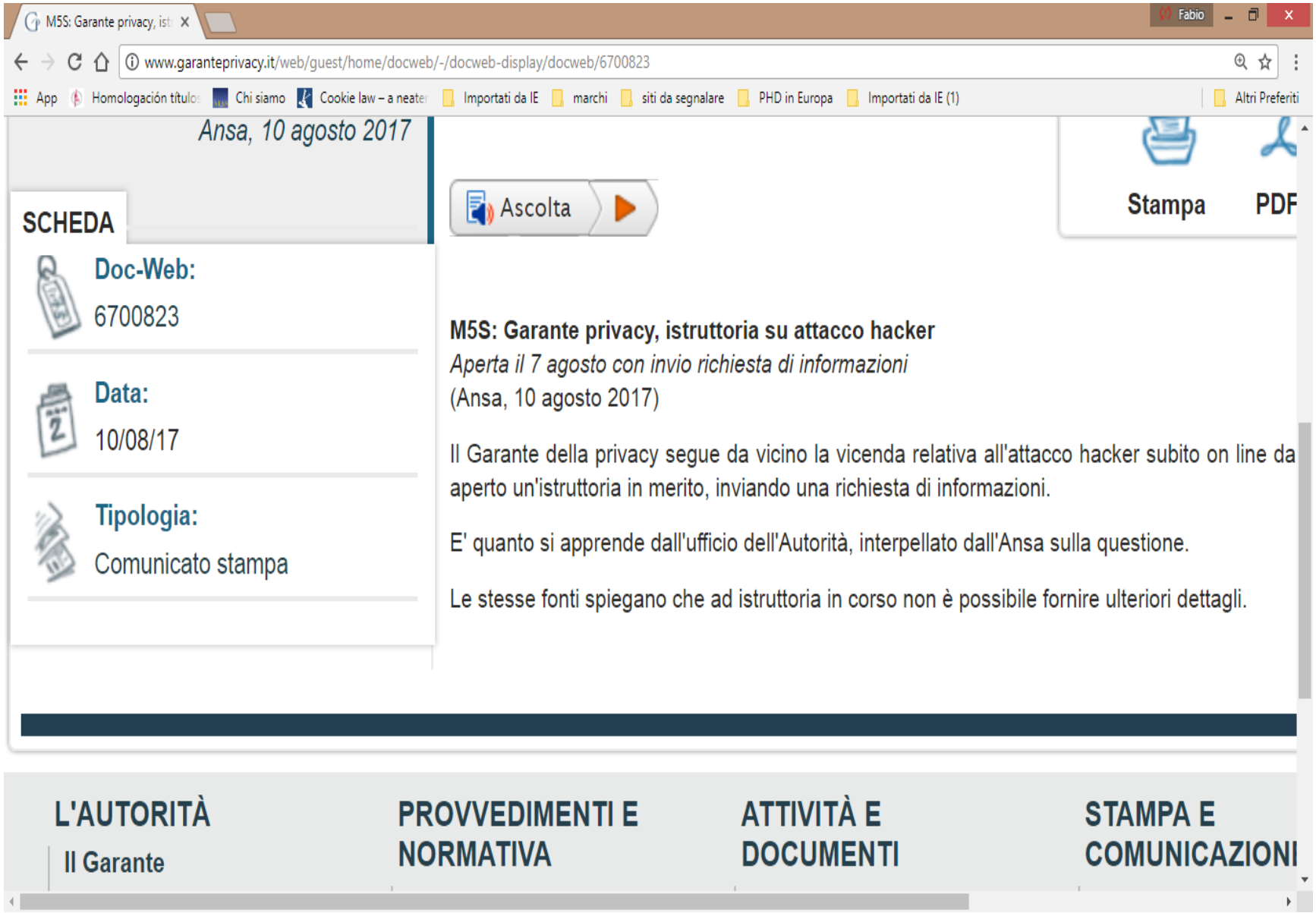
ARCHIVIO STORICO SOTTO OSSERVAZIONE DELLA AUTORITA' DI CONTROLLO

Casistica di data breach



Coinvolti dati personali relativi a 400.000 clienti

Casistica di data breach



Casistica di data breach

Yahoo violata ancora: trafugati i dati di un miliardo di account

L'azienda ha svelato un altro massiccio data breach, identificato grazie al lavoro delle forze dell'ordine. Gli hacker avrebbero prelevato nomi, indirizzi email, numeri di telefono, date di nascita, password crittografate, domande e risposte di sicurezza. I pirati avrebbero inoltre creato cookie speciali per entrare nei profili personali senza utilizzare chiavi d'accesso.

Pubblicato il 15 dicembre 2016 da Alessandro Andreoli



Non c'è pace per Yahoo. Dopo aver svelato solo a settembre un attacco hacker vecchio di almeno due anni, che aveva portato alla compromissione di circa 500 milioni di account, ieri l'azienda ha confermato un'altra intrusione nei propri sistemi informatici. A essere trafugate, questa volta, sarebbero le informazioni

Casistica di data breach

FURTO NOTTURNO SCOPERTO STAMATTINA

Ladri nel palazzo comunale di Aprilia: rubate anche le carte di identità

A+ | A− | 24 febbraio 2017, ore 08:52 Condividi



Casistica di data breach

CORRIERE DELLA SERA

ROMA / CRONACA

3

367

LITORALE

Fiumicino, attacco hacker al Comune Cancellati i database del «sociale»

Il virus giunto per mail con richiesta di soldi in cambio dei dati. Sparite le graduatorie delle case popolari e i back-up. Gonnelli: caso sospetto. Montino: danni gravi



Casistica di data breach

Albano, furto in Comune: rubate 970 carte d'identità



Ennesimo colpo grosso all'ufficio Anagrafe del Comune di Albano dove, in nottata, sono state portate via 970 carte di identità, 500 euro in contanti e un cospicuo numero di valori bollati. Dopo l'analogo furto che ai primi di agosto fruttò un

Casistica di data breach

Articolo pubblicato sull'Unione Sarda 02 febbraio 2017.

PULA

Attacco hacker al Comune: colpa degli antivirus gratis

«Ci chiediamo perché il Comune non protegga in maniera adeguata il sistema informatico dei propri uffici: è inaccettabile affidarsi ad antivirus scaricati gratuitamente da internet». Nei giorni scorsi un potente virus ha attaccato la rete informatica comunale, creando non pochi disagi. L'attacco sarebbe partito da un computer del settore ragioneria: un con- dei dati dei computer comunali, composta da dati e documenti sensibili, ci siano solo antivirus *freeware* - dice Emanuele Olla, del gruppo Libertas - vorremmo sapere perché non è stata presa in considerazione l'ipotesi di acquistarne altri capaci di mettere al riparo la rete da spiacevoli soprese. A volte si utilizza il denaro per iniziative di cui si potrebbe fare a meno e

Casistica di data breach



Home › Aprilia › Aprilia, gruppo di hacker attacca pc di un'azienda e chiede il riscatto...

APRILIA CRONACA LATINA

Aprilia, gruppo di hacker attacca pc di un'azienda e chiede il riscatto per restituire i file

Le nuove frontiere del rapimento 2.0

23 gennaio 2017

Casistica di data breach

Il Mattino > Salerno >

Attacco hacker a un'azienda alterata la gamma di prodotti



Continua a mietere vittime, nel Salernitano, il potente virus informatico "Cryptlocker", in grado di inibire pc e server dell'ignaro utente di turno. Per sbloccare il tutto, il "ransomware", letteralmente "riscatto della merce", chiede una somma di denaro da pagare entro un termine perentorio, spesso accompagnato da un conto alla rovescia sul desktop. Ma, il più delle volte – avvertono gli esperti di sicurezza informatica – pur pagando, non si è certi di rientrare in possesso dei propri archivi.

Casistica di data breach

Ladri senza scrupoli. Furto all'ospedale di Siena, rubato supporto con dati di pazienti e di ricerca

By **Redazione** - 05/06/2017 182 0

SHARE Facebook Twitter G+



Regolamento europeo 2016/679/Ce
WannaCry e l'art. 33



Definiamo «data breach»

La trasmissione, comunicazione o comunque l'apprensione non autorizzata di informazioni [sensibili] ad una parte non è autorizzata.

Il regolamento definisce violazione dei dati personali (art. 4):

La violazione di sicurezza che comporta <u>accidentalmente</u> 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.

Regolamento europeo 2016/679/Ce
Violazione dei dati – art. 4

Come si notifica?

Quando è obbligatorio notificare? (criticità)

Il Regolamento Europeo n. 679/2016

Il Regolamento prevede un sistema di notifica a seconda del rischio associato alla violazione:

1) all'autorità di controllo (art. 33 del GDPR);

2) ai soggetti interessati dalla violazione (art. 34 del GDPR).

Il Regolamento Europeo n. 679/2016 Quando comunicare all'Autorità di controllo?

Considerando 85

Il titolare del trattamento dovrebbe comunicare all'Autorità di controllo in caso la violazione presenti rischi per i diritti e libertà



AI SENSI DELL'ART. 33 CO. 1 E' ESCLUSA LA NOTIFICAZIONE QUANDO SI PUÒ DIMOSTRARE CHE IL

RISCHIO È IMPROBABILE

Il Regolamento Europeo n. 679/2016 Quando comunicare all'Autorità di controllo?

AI SENSI DELL'ART. 33 CO. 1 E' ESCLUSA LA NOTIFICAZIONE QUANDO SI PUÒ DIMOSTRARE CHE

IL RISCHIO È IMPROBABILE



DOCUMENTARE TALE VALUTAZIONE NELL'INVENTARIO DELLE VIOLAZIONI DEI DATI (ART. 32 BIS COMMA 7 C.D.P.)

Il Regolamento Europeo n. 679/2016 Quando comunicare all'interessato?

Considerando 86

Il titolare del trattamento dovrebbe comunicare all'**interessato** la violazione dei dati personali qualora questa violazione sia suscettibile di presentare **UN RISCHIO ELEVATO di pregiudizio per i diritti e le libertà della persona fisica**.

CRITERIO DELL'IMPATTO SIGNIFICATIVO

Il Regolamento Europeo n. 679/2016
Impatto significativo

Il Considerando n. 85

Una violazione dei dati personali può, **se non affrontata in modo adeguato e tempestivo**, provocare:

1. perdita del controllo dei dati personali;
2. limitazione dei diritti delle persone;
3. discriminazione;
4. furto o usurpazione d'identità;
5. perdite finanziarie;
6. pregiudizio alla reputazione;
7. o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il Regolamento Europeo n. 679/2016

Art .33 – Notifica di violazioni dei dati all'autorità di controllo (1)

Termine **di 72 ore per informare** l'Autorità di Controllo dell'avvenuta violazione (o motivi di ritardo)

Contenuto minimo della notifica:

1) La descrizione della natura della violazione;
2) Il numero e le categorie dei dati interessati (se disponibili);
3) Il nome del responsabile della protezione dei dati;
4) Le probabili conseguenze della violazione;
5) Le misure adottate per porvi rimedio e/o attenuarne gli effetti negativi.

Il Regolamento Europeo n. 679/2016

Art .34 – Comunicazione di una violazione dei dati personali all'interessato (1)

Non si menziona un termine preciso entro il quale adempiere, ma il legislatore prevede che questa debba avvenire "**senza ingiustificato ritardo**".

L'obbligo di comunicazione all'interessato si attiva nei casi più gravi, in cui dalla violazione possano derivare **rischi elevati per i diritti e le libertà delle persone fisiche**.

Il Regolamento Europeo n. 679/2016

Art .34 – Comunicazione di una violazione dei dati personali all'interessato (2)

La notifica delle violazioni deve almeno:

a) 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;

b) descrivere le probabili conseguenze della violazione dei dati personali;

c) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione all'interessato deve essere formulata con un linguaggio semplice e chiaro e deve descrivere la natura della violazione dei dati personali.

Gestione della procedura del data breach

E’ importante che i Titolari del trattamento procedano a un'adeguata pianificazione adottando e attuando misure tecniche ed organizzative adatte per garantire un livello di sicurezza appropriato rispetto ai rischi individuati.

Quindi sarà necessario:

1) idoneo quadro di gestione dei rischi (valutazione dei rischi e valutazione di impatto);
2) corretta tenuta del Registro dei Trattamenti (anche se non obbligatorio);
3) Corretta tenuta di Inventario delle Violazioni dei dati (art. 32 bis co. 7 C.d.P. e previsto dai provv. Garante privacy in materia)
4) **istituire preventivamente piani appropriati per il trattamento (mitigazione dei rischi) delle violazioni dei dati personali;**

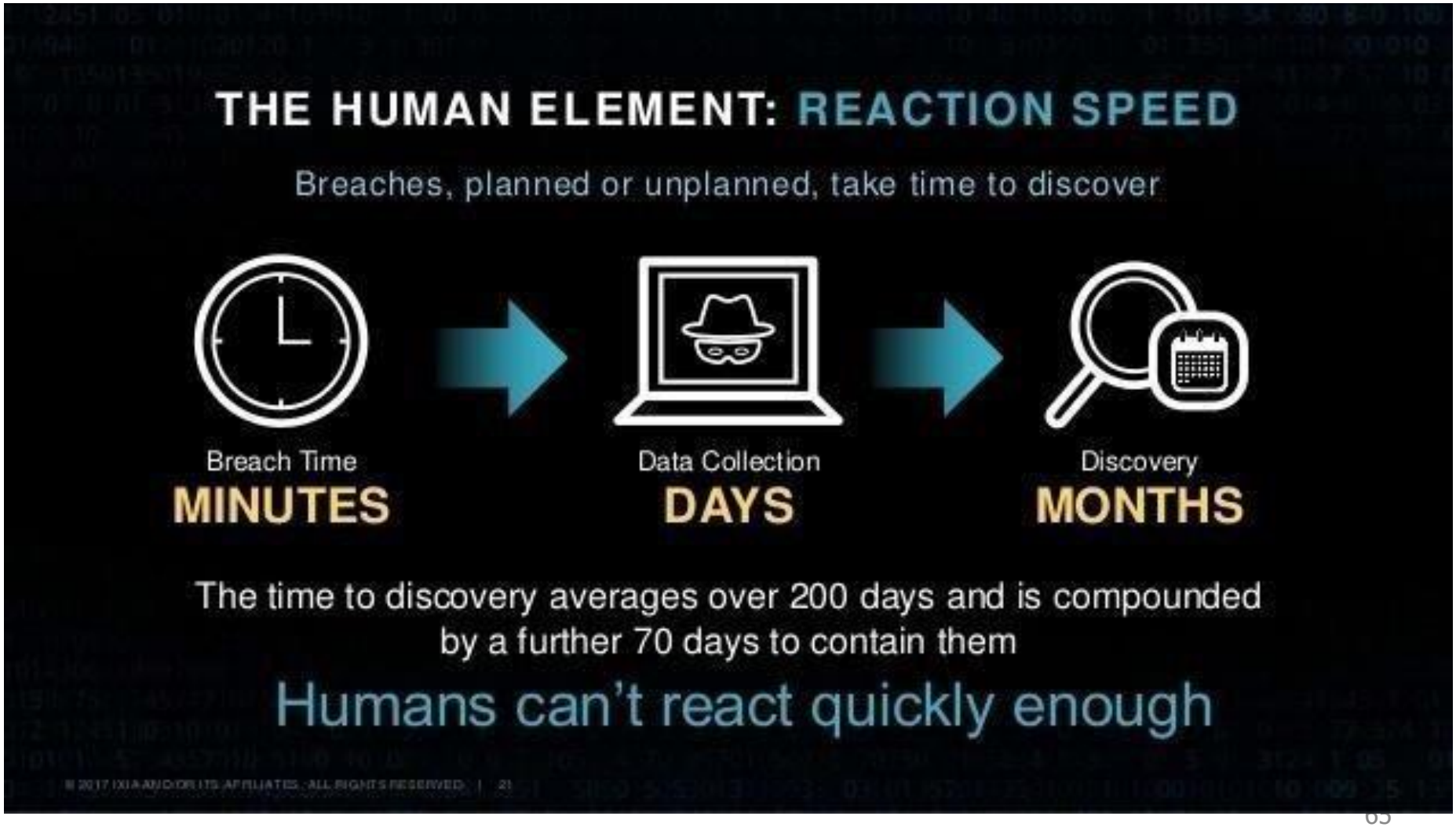
Sanzioni
Criteri per la determinazione dell'importo

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso **effettive**, **proporzionate** e **dissuasive**.

Sanzioni
Massimo edittale

In caso di data breach in base all'art. 83 del GDPR la sanzione pecuniaria è fino a 10 ml di euro o del 2% del fatturato mondiale annuo dell'impresa se l'importo è superiore

Regolamento europeo 2016/679/Ce
Tempi di scoperta e reazione al data breach



Regolamento europeo 2016/679/Ce
regime di esenzione data breach

Nel codice della Privacy all'art. 32 bis è previsto al comma 3 che un esenzione delle **comunicazione dei dati a «contrante e altre persona»** se i dati sono resi inintelligibili tramite misure di protezione: *impatto sensibile/rischi di arrecare pregiudizio*

Nel GDPR al comma terzo la lett. a) ha un contenuto analogo

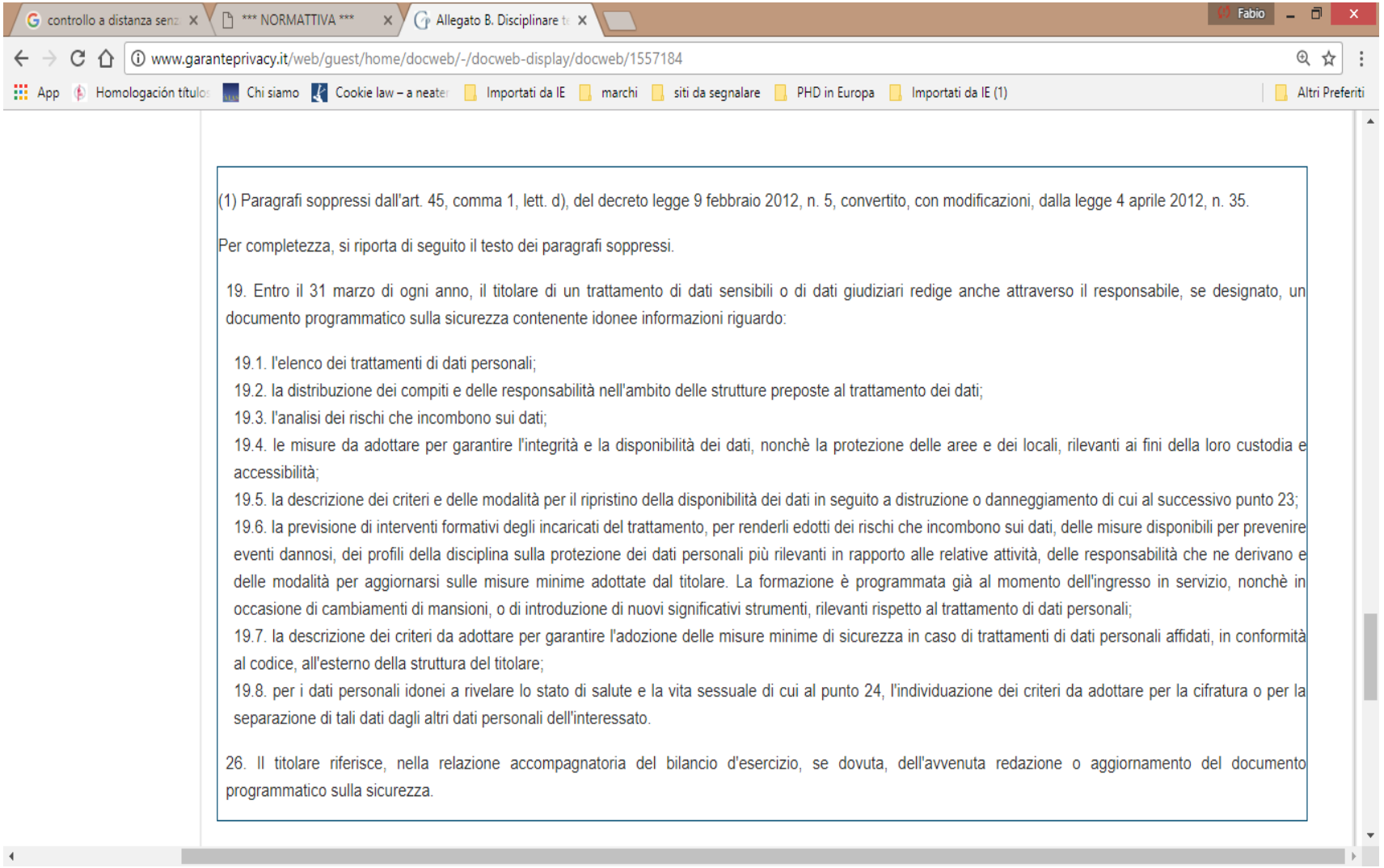
Aggiunta importante presente nel regolamento e che garantisce un'esenzione anche in caso di violazione dei dati:

«il titolare del trattamento **ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e libertà fondamentali**»

Passaggio dal Documento Programmatico per la sicurezza (DPS)

al Registro delle attività di trattamento ex art. 30 GDPR

Regolamento europeo 2016/679/Ce
DOCUMENTO PROGRAMMATICO PER LA SICUREZZA - DPS



(1) Paragrafi soppressi dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. 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. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Regolamento europeo 2016/679/Ce
Dal DPS a RdA

Il registro dei trattamenti può essere un documento più sintetico del DPS

TITOLARE E RAPPRESENTANTE (art. 30 gdpr):

a)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 responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) 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;
f) ove possibile, **i termini ultimi previsti per la cancellazione delle diverse categorie di dati**;
g) ove possibile, **una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1**.

Regolamento europeo 2016/679/Ce
Dal DPS a RdA

Il registro dei trattamenti può essere un documento più sintetico del DPS?

TITOLARE E RAPPRESENTANTE:

R.d.A. è simile al DPS semplificato o alla notificazione ex art. 38? Cosa può essere eliminato rispetto al **DPS ordinario**

19.2 La distribuzione dei compiti e delle responsabilità (rif. Organigramma)
19.3 Analisi dei rischi
19.6 Previsione di interventi formativi degli incaricati del trattamento

Il R.d.A. è richiesto un contenuto minimo come asserito dal Garante privacy nulla impedisce che il R.d.A. contenga anche allegati o sezioni che vadano oltre lo stretto
Indispensabile anche perché rappresenta lo strumento più critico per dimostrare la
Conformità in un ottica di accountability

Regolamento europeo 2016/679/Ce
Dal DPS a RdA

Il DPS SEMPLIFICATO CONTENUTO – PUNTO 2.5 - PROVV. 27 NOV. 2008

a) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento;

b) una descrizione generale del trattamento o dei trattamenti realizzati, che permetta di valutare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione vanno precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, nonché i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;

c) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Nel caso in cui l'organizzazione preveda una frequente modifica dei responsabili designati, potranno essere indicate le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità;

d) una **descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta**.

Regolamento europeo 2016/679/Ce
Dal DPS a RdA

TITOLARE E RAPPRESENTANTE:

R.d.A. simile al DPS semplificato? Cosa può essere eliminato rispetto al **DPS ordinario**

Il R.d.A. è richiesto un contenuto minimo come asserito dal Garante privacy nulla impedisce che il R.d.A. contenga anche allegati o sezioni che vadano oltre lo stretto indispensabile anche perché rappresenta lo strumento più critico per dimostrare la conformità in un ottica di accountability

Regolamento europeo 2016/679/Ce
Dal DPS a RdA

TITOLARE E RAPPRESENTANTE:

R.d.A. simile al DPS semplificato? Cosa può essere eliminato rispetto al **DPS ordinario**

PERCOLI

Come per l'autocertificazione: documento sintetico per eccellenza
Un registro delle attività sintetico potrebbe comportare delle dichiarazioni false e discordanti se non supportato adeguatamente da documentazione

Un dichiarazione contenuta in autocertificazione o in un documento che deve provare la verità di alcune circostanze di fatto (p.e. quali misure specifiche sono state adottate) che successivamente viene trasfusa in un verbale dell'organo di accertamento diventa falso ideologico di privato in atto pubblico ex articolo 483 c.p.

Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Grazie per l'attenzione

Fabio Di Resta

I materiali didattici saranno disponibili su
www.fondazioneifel.it/formazione

Twitter Facebook YouTube