Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

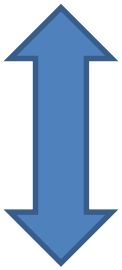
L'impatto sui Comuni del regolamento europeo sulla privacy

Avv. Fabio Di Resta

3 maggio 2018

La protezione dei dati personali

Protezione dei dati personali

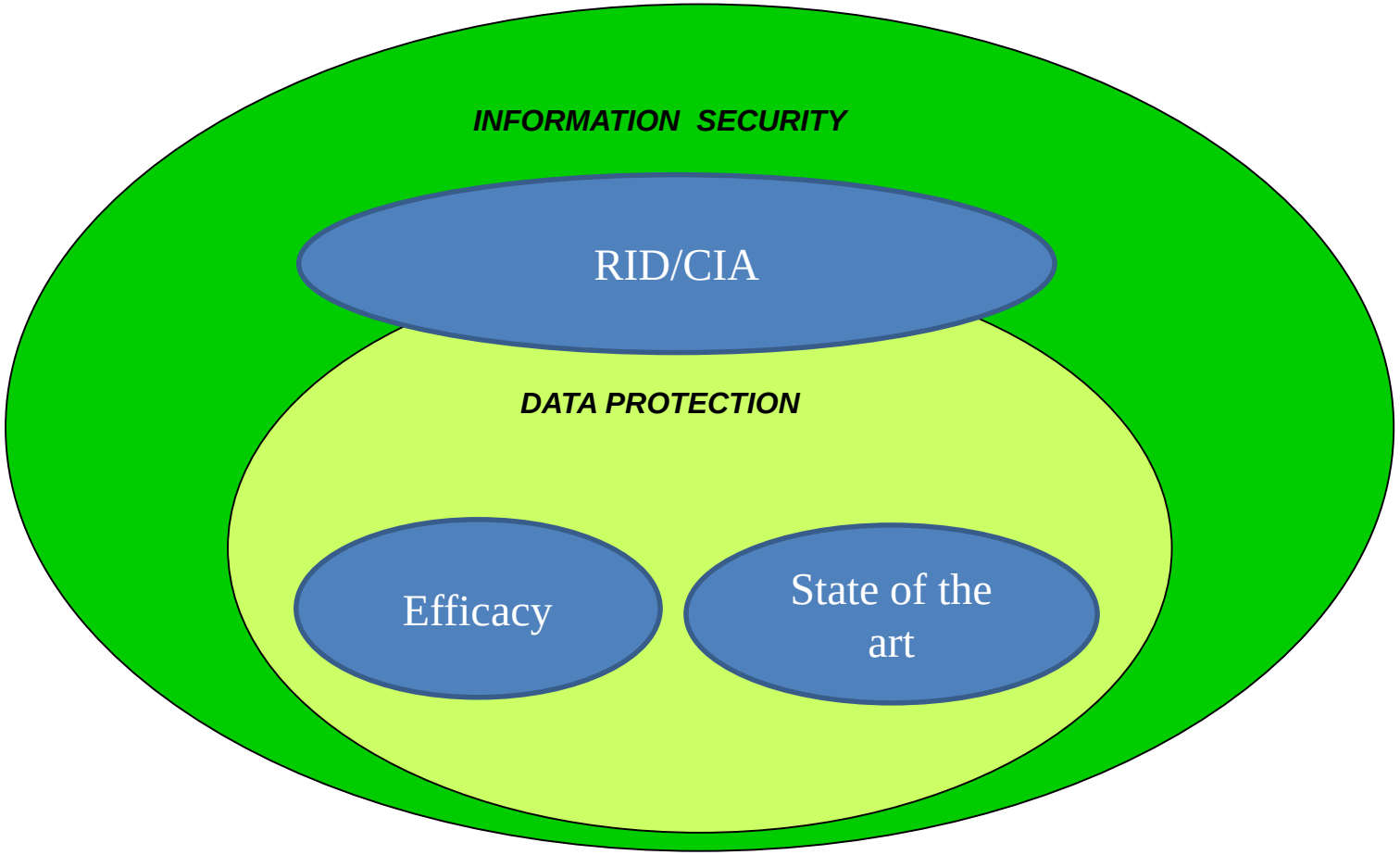


sicurezza fisica – logica ed organizzativa

La protezione dei dati personali
Modello Codice della Privacy

Formazione per i Comuni
IFEL Fondazione ANCI

GDPR - Modello di protezione dei dati personali più maturo

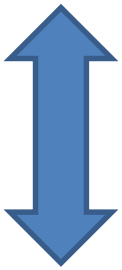


Formazione IFEL per i Comuni

IFEL Fondazione ANCI

La protezione dei dati personali
CODICE DELLA PRIVACY

Protezione dei dati personali

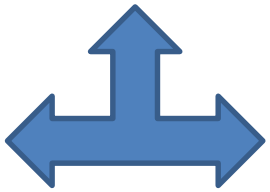


Privacy

La protezione dei dati personali nel GDPR

Approccio proattivo nella sicurezza dei dati personali

Codice della privacy



GDPR

Altre riforme normative in corso

Revisione Convenzione 108/81 – Consiglio d'Europa

Revisione della direttiva 2002/58/Ce – c.d. e-Privacy Directive: **e-privacy Regulation (Titolo X Codice)**

Revisione del regolamento 45/2001 relativo al trattamento dei dati personali da parte delle istituzioni, degli organi e uffici dell'Unione europea (**DPO**)

Il pacchetto di riforma in materia di protezione dei dati

Regolamento Generale sulla Protezione dei Dati personali

Regolamento 2016/679

Direttiva sul trattamento dei dati personali delle persone fisiche a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

Direttiva «Polizia» 2016/680

Regolamento europeo 2016/679/Ce
La riforma normativa europea e le motivazioni

Esigenza di costituire un mercato unico digitale a livello europeo in grado di far fronte alle sfide di un mondo globalizzato ed in grado di rispondere agli utenti in termini di maggiore fiducia: sviluppo tecnologico

la costituzionalizzazione del diritto fondamentale

alla protezione dei dati personali

(l'art. 16 TFUE dopo il Trattato di Lisbona)

frammentazione del quadro normativo (trasposizione disomogenea della Direttiva 95/46 nei diritti nazionali)

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

Regolamento europeo 2016/679/Ce
La riforma normativa e le motivazioni

Esigenza di costituire un mercato unico digitale a livello europeo in grado di far fronte alle sfide di un mondo globalizzato ed in grado di rispondere agli utenti in termini di maggiore fiducia: sviluppo tecnologico

la costituzionalizzazione del diritto fondamentale

alla protezione dei dati personali (l'art. 16 TFUE dopo il Trattato di Lisbona - ex articolo 286 del TCE)

frammentazione del quadro normativo (trasposizione disomogenea della Direttiva 95/46 nei diritti nazionali)

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

Regolamento europeo 2016/679/Ce
La riforma normativa e le motivazioni

la costituzionalizzazione del diritto fondamentale alla protezione dei dati personali – Art. 16 TFUE

«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.»

Regolamento europeo 2016/679/Ce
La riforma normativa e le motivazioni

Esigenza di costituire un mercato unico digitale a livello europeo in grado di far fronte alle sfide di un mondo globalizzato ed in grado di rispondere agli utenti in termini di maggiore fiducia: sviluppo tecnologico

la costituzionalizzazione del diritto fondamentale

alla protezione dei dati personali

(l'art. 16 TFUE dopo il Trattato di Lisbona)

frammentazione del quadro normativo (trasposizione disomogenea della Direttiva 95/46 nei diritti nazionali)

Regolamento europeo 2016/679/Ce
LA STRUTTURA NORMATIVA

Capo I disposizioni generali – artt. da 1 a 4

Capo II Principi – artt. da 5 a 11

Capo III Diritti dell'interessato – artt. da 12 a 23

Capo IV Titolare del trattamento e responsabili – artt. da 24 a 43

Capo V Trasferimento di dati verso paesi terzi o organizzazioni internazionali – artt. da 44 a50

Capo VI Autorità di controllo – artt. da 51 a 59

Capo VII Cooperazione e Coerenza – artt. da 60 a 76

Capo VIII Mezzi di ricorso, responsabilità e sanzioni – artt. da 77 a 84

Regolamento europeo 2016/679/Ce
LA STRUTTURA NORMATIVA

Capo IX disposizioni relative a specifiche situazioni di trattamento – artt. da 85 a 91

Capo X atti delegati e atti di esecuzione – artt. da 92 a 93

Capo XI Disposizioni finali – artt. da 94 a 99

Regolamento europeo 2016/679/Ce

ANALISI DEL GDPR

Regolamento europeo 2016/679/Ce
Oggetto e finalità

1.Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2.Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3.La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Regolamento europeo 2016/679/Ce
Ambito di applicazione materiale
Art. 2

1.Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2.Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE (nota: disposizioni specifiche PESC); c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Direttiva 95/46/Ce
Campo di applicazione – art. 3

1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali;

- effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

- **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.**

Regolamento europeo 2016/679/Ce
Ambito di applicazione territoriale – Art. 3

1.Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.(nota: considerando 22; norma anti-elusione)

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. (nota: considerandi 23 e 24)

3.Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico. (considerando 25)

Regolamento europeo 2016/679/Ce
Ambito di applicazione territoriale

1.Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.(nota: considerando 22)

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. (nota: considerandi 23 e 24; extraterrialità del diritto europeo: punti di forza e di debolezza dei rapporti istituzionali internazionali)

3.Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico. (considerando 25)

Regolamento europeo 2016/679/Ce
Ambito di applicazione territoriale

1.Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

(nota: considerando 22)

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. (nota: considerandi 23 e 24)

3.Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico. (considerando 25)

Regolamento europeo 2016/679/Ce
Nuove definizioni

Ai fini del presente regolamento s'intende per: 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (**nota: categorie particolari di dati personali vs dati sensibili**)

Regolamento europeo 2016/679/Ce
Nuove definizioni

3) «limitazione di trattamento»: **il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;**

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Regolamento europeo 2016/679/Ce
Nuove definizioni

5) **«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;**

Regolamento europeo 2016/679/Ce
Nuove definizioni

11)«consenso dell'interessato»: 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;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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;

Regolamento europeo 2016/679/Ce
Nuove definizioni

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;

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;

Regolamento europeo 2016/679/Ce
Nuove definizioni

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della **sua amministrazione centrale nell'Unione**, salvo che **le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale**;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua **amministrazione centrale nell'Unione** o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento

Regolamento europeo 2016/679/Ce

INFORMATIVA E CONSENSO NEL REGOLAMENTO

PRINCIPALI NOVITA'

Regolamento europeo 2016/679/Ce
Condizioni del consenso - Art. 7 (cons. 32 gdpr)

1.Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere **in grado di dimostrare che l'interessato** ha prestato il proprio consenso al trattamento dei propri dati personali.

2.Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, 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. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante. **(nota: assunto ricorrente in varie pronunce del Garante privacy)**

3.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 di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Regolamento europeo 2016/679/Ce
Condizioni del consenso

4.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. (nota: assunto ricorrente in varie pronunce del Garante privacy)**

Regolamento europeo 2016/679/Ce
Condizioni applicabili al consenso dei minori
Art. 8

1.Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore **è lecito ove il minore abbia almeno 16 anni**. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

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

Regolamento europeo 2016/679/Ce
Trattamento di categorie particolari di dati personali

Art. 9

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.

(nota: **formalmente si abbandona la nozione di «dato sensibile» e si riprende la nozione di categorie particolari di dati personali già note nelle legge 675/96 abrogata dal d.lgs. 196/2003**)

Regolamento europeo 2016/679/Ce
Diritti dell'interessato – Trasparenza e modalità

Art. 12

1.Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente **ai minori**. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2.Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

Regolamento europeo 2016/679/Ce
Diritti alla portabilità – tempi di riscontro

Art. 12

3.Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, **al più tardi entro un mese dal ricevimento della richiesta stessa**. **Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.** Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. (**Cfr. riscontro/interpello preventivo ai sensi dell'art. 143 del Codice della Privacy 15 gg prorogato fino a 30 gg**)

15 + 15 CdP = max 30 CdP

30 + 60 Gdpr = max 90 Gdpr

Regolamento europeo 2016/679/Ce
Diritti dell'interessato – Trasparenza e modalità

Art. 12

4.Se non ottempera alla richiesta dell'interessato, **il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.**

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 **sono gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) **addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta**; oppure b) rifiutare di soddisfare la richiesta. (**Cfr. provvedimento del Garante privacy, deliberazione 23 dicembre 2004**)

Regolamento europeo 2016/679/Ce
Diritti dell'interessato – Trasparenza e modalità

Art. 12

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6.Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7.Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8.Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Regolamento europeo 2016/679/Ce informativa privacy

Art. 13

1.In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di **contatto del responsabile della protezione dei dati, ove applicabile**; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), **i legittimi interessi perseguiti dal titolare del trattamento o da terzi**; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f)ove applicabile, **l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale** e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Regolamento europeo 2016/679/Ce informativa privacy

Art. 13

2.In aggiunta alle informazioni di cui al paragrafo 1, **nel momento in cui i dati personali sono ottenuti**, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) **il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo**; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, **oltre al diritto alla portabilità dei dati**; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), **l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca**;

Regolamento europeo 2016/679/Ce informativa privacy

Art. 13

d) **il diritto di proporre reclamo a un'autorità di controllo**; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3.Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2. (nota: **nell'informativa ai sensi dell'art. 13 del Codice della Privacy è prevista solo l'indicazione dei diritti dell'interessato secondo l'art. 7**)

Regolamento europeo 2016/679/Ce
Riepilogo «cosa cambia» nell'informativa gdpr

1. Dati di contatto del DPO (non necessario il nome: requisito di conoscibilità esterna del DPO)
2. Periodo di conservazione
3. Portabilità dei dati
4. Diritto di proporre il reclamo
5. Icone standardizzate
6. Revoca del consenso
7. Intenzione di trasferire i dati fuori dall'UE/SEE
8. Specificare se il trattamento è necessario per perseguire il legittimo interesse del titolare o da terzi (marketing diretto anche tramite terzi o prevenzione frodi) (cfr. considerandi nn. 47, 48, 50, 111)
9. Qualora l'informativa riguardi i minori si deve utilizzare un linguaggio chiaro e semplice adatto a loro
10. Eventuali destinatari o categorie di destinatari

Regolamento europeo 2016/679/Ce
Riepilogo «cosa cambia» nell'informativa gdpr

Test dell'interesse legittimo GDPR

«l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine.»

Interesse legittimo Codice della Privacy

«Art. 24. **Casi nei quali può essere effettuato il trattamento senza consenso**:

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato […]»

Regolamento europeo 2016/679/Ce
Riepilogo «cosa cambia» nell'informativa gdpr

Test dell'interesse legittimo

- Costituisce parimenti legittimo interesse del titolare del trattamento che tratta dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.

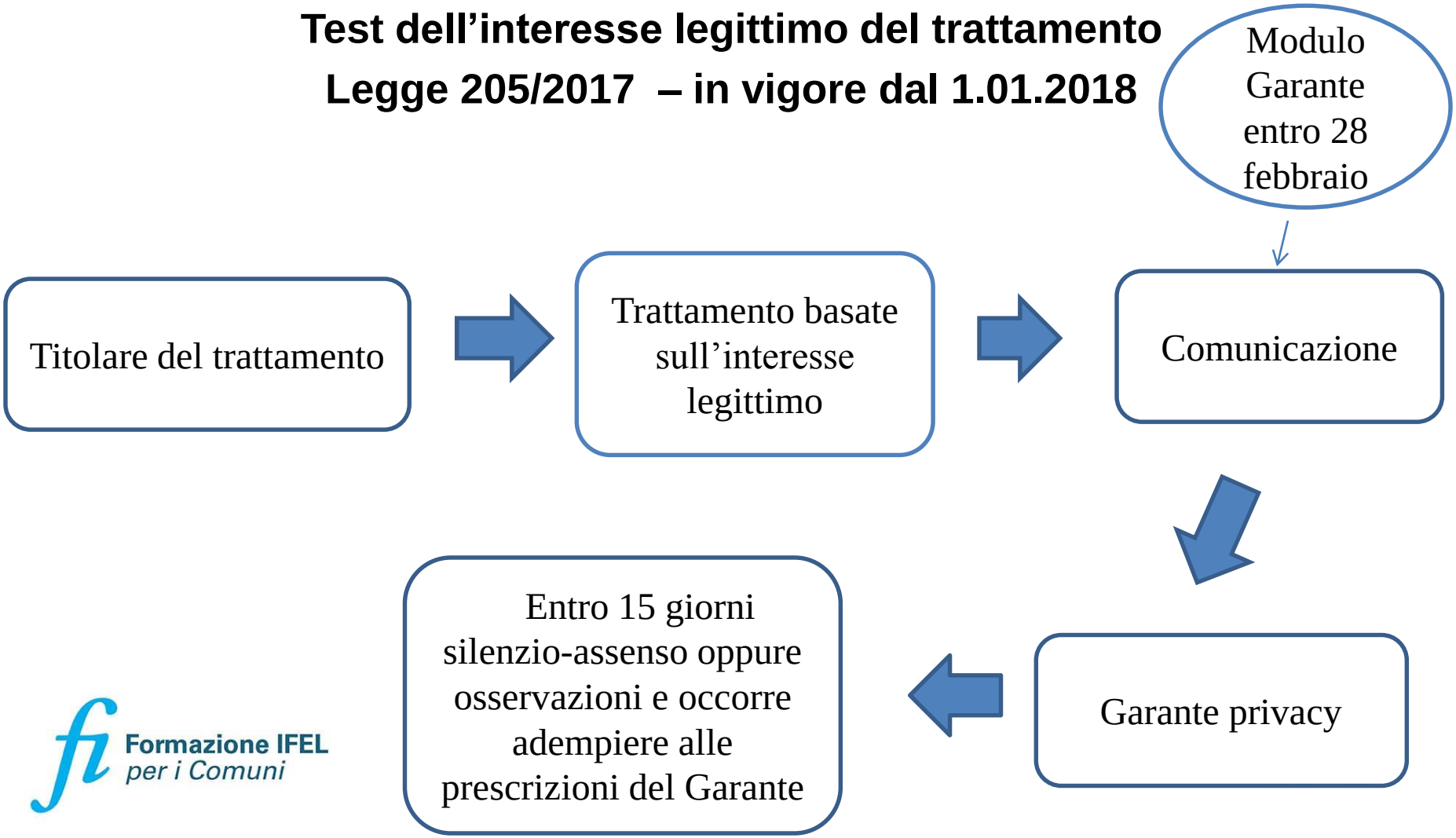
- la sicurezza delle reti e dell'informazione
  (**tradizionale dicotomia sicurezza e privacy**)

- possibili reati o minacce alla sicurezza pubblica

- Trattamento dei dati personali all'interno di gruppo di imprese per finalità contabili-amministrative

Regolamento europeo 2016/679/Ce
Riepilogo «cosa cambia» nell'informativa gdpr

Test dell'interesse legittimo del trattamento
Legge 205/2017 – in vigore dal 1.01.2018



Formazione IFEL per i Comuni

Regolamento europeo 2016/679/Ce
Diritto di accesso

Art. 15

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, **il periodo di conservazione dei dati personali** previsto oppure, se non è possibile, **i criteri utilizzati per determinare tale periodo**; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento

Regolamento europeo 2016/679/Ce
Diritto di accesso

Art. 15

f) il diritto di proporre reclamo a un'autorità di controllo; g) **qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine**; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. (**nota: Cfr. art. 7 del Codice delle Privacy manca uno specifico riferimento all'origine dei dati**)

Regolamento europeo 2016/679/Ce
Diritto alla cancellazione (diritto all'oblio)

Art. 17

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

Regolamento europeo 2016/679/Ce
Diritto alla cancellazione (diritto all'oblio)

Art. 17

d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2.Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. 3.I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione;

[…]

Regolamento europeo 2016/679/Ce
Diritto di limitazione di trattamento

Art. 18

1.L'interessato ha il diritto di ottenere dal titolare del trattamento la **limitazione del trattamento** quando ricorre una delle seguenti ipotesi: a) **l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria**; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

[...]

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

INFORMATIVA ONLINE

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

1. INFORMATIVA GENERALE SERVIZI ONLINE COMUNE DI XY

Informativa sulla privacy

Con l'entrata in vigore del D.Lgs 196/2003, " Codice in materia di protezione dei dati personali ", recante disposizioni per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, XY è tenuta a fornire alcune informazioni riguardanti l'utilizzo dei dati personali. Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità e trasparenza al fine di tutelare la Sua riservatezza e i Suoi diritti.

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

2. INFORMATIVA GENERALE SERVIZI ONLINE COMUNE DI XY

Informativa

Ai sensi dell'art.13 del D.Lgs. n.196/2003 "Codice in materia di protezione dei dati personali" Le forniamo quindi le seguenti informazioni.

I dati personali forniti con il presente documento – nonché quelli già in possesso dell'Ente - saranno trattati solo ed esclusivamente per fini istituzionali allo scopo di abilitare l'utente, che lo richiede, alla fruizione dei servizi on-line erogati nel sito www.comune.XY.it nell'area Servizi on-line.

Il trattamento dei dati per la suddetta finalità:

a) è realizzato attraverso operazioni o complessi di operazioni indicate dall'art. 4 del D.Lgs. n. 196/2003;

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

3. INFORMATIVA GENERALE SERVIZI ONLINE COMUNE DI XY

b) è effettuato con l'ausilio di mezzi elettronici e/o modalità volte ad assicurare un livello minimo di protezione dei dati ed idonee a garantirne la sicurezza e la riservatezza, nel rispetto di quanto definito negli articoli n.33 e seguenti del D.Lgs 30 giugno 2003 n.196;

L'eventuale rifiuto di conferire i dati personali da parte dell'interessato comporta l'impossibilità, per lo stesso, di usufruire dei servizi erogati on-line per i quali si prevede una registrazione identificata.

Nel caso in cui l'utente scelga un servizio, gestito in tutto o in parte da altro soggetto, i suoi dati verranno comunicati, come richiesto e/o previsto, ai singoli gestori che opereranno come Titolari per il trattamento connesso all'erogazione dei servizi di propria competenza; i dati identificativi e le modalità previste possono essere richieste al responsabile del trattamento dei dati.

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

5. INFORMATIVA GENERALE SERVIZI ONLINE COMUNE DI XY

In relazione al trattamento dei dati raccolti, il soggetto interessato potrà esercitare i diritti previsti dall'art. 7 – 8 – 9 – 10 del suddetto D.Lgs. 196/2003. In particolare l'interessato può ottenere dal titolare o dai responsabili del trattamento dei dati:

- la conferma dell'esistenza o meno di propri dati personali e la loro messa a disposizione in forma intelligibile;

- avere conoscenza dell'origine dei dati, nonché della logica e delle finalità su cui si basa il trattamento;

- ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge, nonché l'aggiornamento, la rettificazione o l'integrazione dei dati;

- opporsi, per motivi legittimi, al trattamento.

Il titolare del trattamento dei dati personali è il Sindaco di XY.

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

CASE STUDY

6. INFORMATIVA GENERALE SERVIZI ONLINE COMUNE DI XY

I responsabili del trattamento dei dati sono individuati nei Dirigenti di livello apicale delle strutture, come da ordinanza del Sindaco, in relazione ai diversi procedimenti attivabili attraverso i servizi on line sul Portale di XY.

ESTRATTO DI INFORMATIVA COOKIE

Il titolare del trattamento dei dati personali è il Sindaco di XY. I responsabili del trattamento dei dati sono individuati nei Dirigenti di livello apicale delle strutture, come da ordinanza del Sindaco, in relazione ai diversi procedimenti attivabili attraverso i servizi on-line sul Portale di XY.

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

Domande:

Manca qualcosa in base all'art. 13 Codice della Privacy?

E' conforme al Codice e al GDPR?

Manca qualcosa in base all'art. 12 del GDPR?

Regolamento europeo 2016/679/Ce
CODICE DELLA PRIVACY

Domande:

Manca qualcosa in base all'art. 13 Codice della Privacy?

Osservazioni

Finalità specifiche del trattamento tramite il portale non sono menzionate

Le categorie di soggetti ai quali vengono comunicati i dati degli utenti non sono indicate né reperibili (art. 13 lett. f) reperibilità elenco responsabili)

Il titolare sebbene identificato, si badi bene «Sindaco del Comune»

I contatti per l'accesso ex art. 7 C.d.P. per rivolgersi al titolare non compaiono, nessun responsabile addetto al riscontro

Regolamento europeo 2016/679/Ce
Manca qualcosa rispetto al gdpr

INFORMATIVA COMUNE XY

1. **Dati di contatto del DPO** (non necessario il nome: requisito di conoscibilità esterna del DPO)
2. **Periodo di conservazione**
3. **Portabilità dei dati, LIMITI SOGGETTI PUBBLICI**
4. **Diritto di proporre il reclamo**
5. Icone standardizzate
6. **Revoca del consenso**
7. Intenzione di trasferire i dati fuori dall'UE/SEE
8. Specificare se il trattamento è necessario per perseguire il legittimo interesse del titolare o da terzi, NO BASE GIURIDICA PER SOGGETTI PUBBLICI X FINALITA' ISTITUZIONALI (marketing diretto anche tramite terzi o prevenzione frodi) (cfr. considerandi nn. 47, 48, 50, 111)
9. **Qualora l'informativa riguardi i minori si deve utilizzare un linguaggio chiaro e semplice adatto a loro**
10. Eventuali destinatari o categorie di destinatari

Regolamento europeo 2016/679/Ce
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

DATA PROTECTION BY DESIGN

DATA PROTECTION BY DEFAULT

Regolamento europeo 2016/679/Ce
Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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.

Regolamento europeo 2016/679/Ce
Protezione dei dati fin dalla progettazione e protezione 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**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information Commissioner Officer - ICO

Benefits of taking a ‘privacy by design’ approach

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust.

Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Increased awareness of privacy and data protection across an organisation.

Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.

Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

Privacy by Design (PbD) was developed by the Information and Privacy Commissioner of Ontario, Canada, *Dr. Ann Cavoukian*, back in the‘90s. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must **become an organization’s default mode of operation**.

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

The 7 Foundational Principles of Privacy by Design have proven to be a valuable resource for individuals and organizations around the world. Since the passing of this international resolution, the 7 Foundational Principles of Privacy by Design have been translated **into 31 official languages**. The objectives of Privacy by Design — ensuring privacy protection and gaining personal control over one's own information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles:

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

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

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

6. **Visibility and Transparency** — Keep it Open Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. **Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify**. (Nota: trasparenza come possibilità di verificare la qualità dei dati trattati, finalità, modalità del trattamento, ecc., ecc.)

Regolamento europeo 2016/679/Ce
Un approccio alla Privacy by Design

Information & Privacy Commissioner of Ontario

The 7 Foundational Principles

7. **Respect for User Privacy** — Keep it User-Centric Above all, Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. **Keep it user-centric**.

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

La piattaforma consente di accedere ad informazioni specifiche

Consente agli utenti di interagire tra loro tramite chat

Gli utenti si registrano alla piattaforma inserendo dati anagrafici dati personali identificativi inclusi tra i campi

obbligatori:

Email

Numero di cellulare

l'informativa privacy riporta esclusivamente tra le finalità solo quelle relative ai servizi essenziali di gestione della piattaforma

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

CASE STUDY

PRIVACY BY DESIGN
CONDIZIONI DI LICEITA' DEL TRATTAMENTO

Realizzazione di un Progetto di piattaforma web

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

Dopo qualche anno la piattaforma ha ottenuto successo e della società terze sono interessate ad effettuare marketing mirato sugli utenti della piattaforma, tuttavia i proprietari del sito scoprono che le informative e i relativi consensi non sono adeguati ovvero non conteneva le garanzie previste per effettuare marketing mirato sulle esigenze degli utenti

Come si può rimediare?

Ci sono soluzioni?

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

Come si può rimediare?

L'art. 130 co. 4 Codice della Privacy (c.d. soft spam) ci può aiutare?

Ma perché non ho avuto un approccio proattivo quando ho effettuato l'investimento iniziale?

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Quando posso ricorrere all'interesse legittimo per il marketing diretto?

L'art. 130 co. 4 Codice della Privacy (c.d. soft spam)

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

Ma perché non ho avuto un approccio proattivo quando ho effettuato l'investimento iniziale?

Regolamento europeo 2016/679/Ce scenario applicativo Privacy by Design

Realizzazione di un Progetto di piattaforma web

Come si può rimediare?

Se i dati degli utenti vengono trasferiti fuori dall'EU/SEE?

Regolamento europeo 2016/679/Ce
Violazione dei dati – applicazione estesa

VIOLAZIONE DEI DATI – DATA BREACH

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

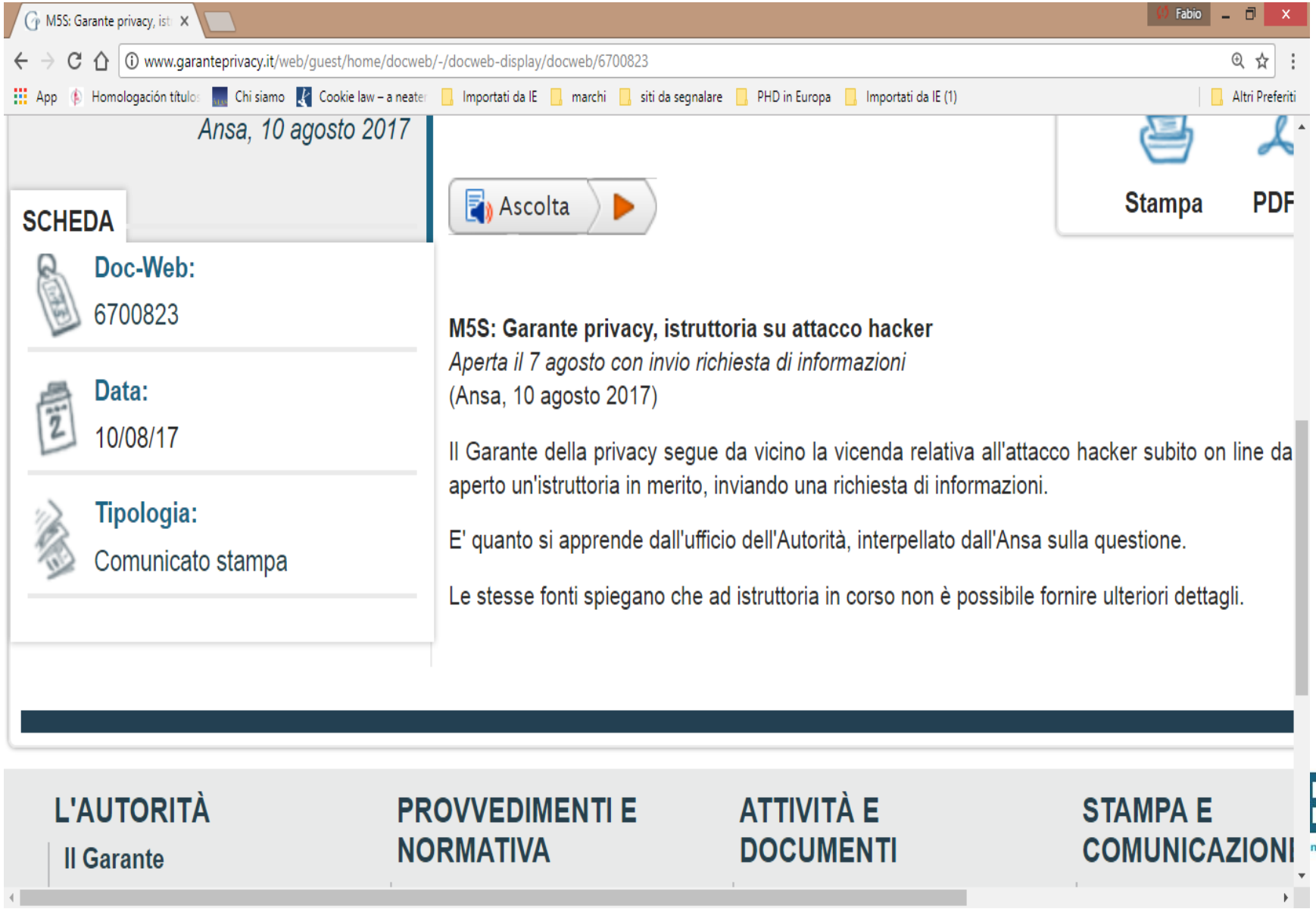
ARCHIVIO STORICO SOTTO OSSERVAZIONE DELLA AUTORITA' DI CONTROLLO

Formazione per i Comu

IFEL Fondazione ANCI

Casistica di data breach

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

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[illegible] 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

Patient records stolen in computer breach at Torrance Memorial Medical Center

Torrance Memorial Medical Center reported that a data breach occurred in April 2017. File photo. (Thomas R. Cordova/Daily Breeze/SCNG)

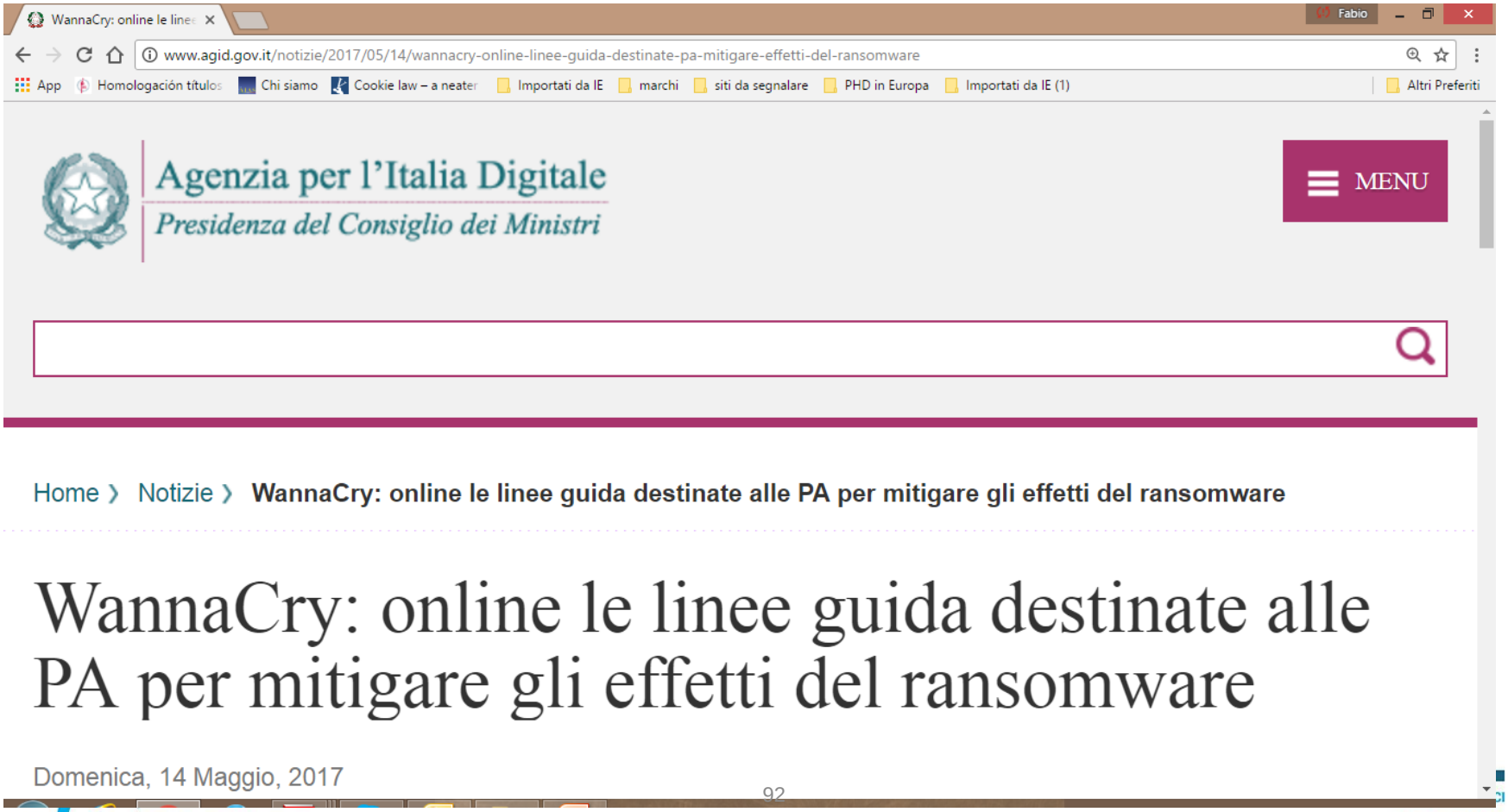
Casistica di data breach

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 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**»

Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Grazie per l'attenzione

Avv. Fabio Di Resta
avvdiresta@direstalawyers.eu

Avvocato - LL.M. - ISO 27001 Security Lead Auditor
Di Resta Lawyers – Roma - Latina - www.direstalawyers.eu
Docente universitario a contratto Master di I livello Gestione del personale e Corso di Alta formazione in antiriciclaggio Università la Sapienza di Roma, Facoltà di Economia
Docente universitario a contratto Master di II livello «I nuovi Professionisti privacy» Università Niccolò Cusano di Roma, Facoltà di Giurisprudenza
Presidente del Centro europeo per la privacy – EPCE