Introduzione alla protezione dei dati personali

Altrui e propri

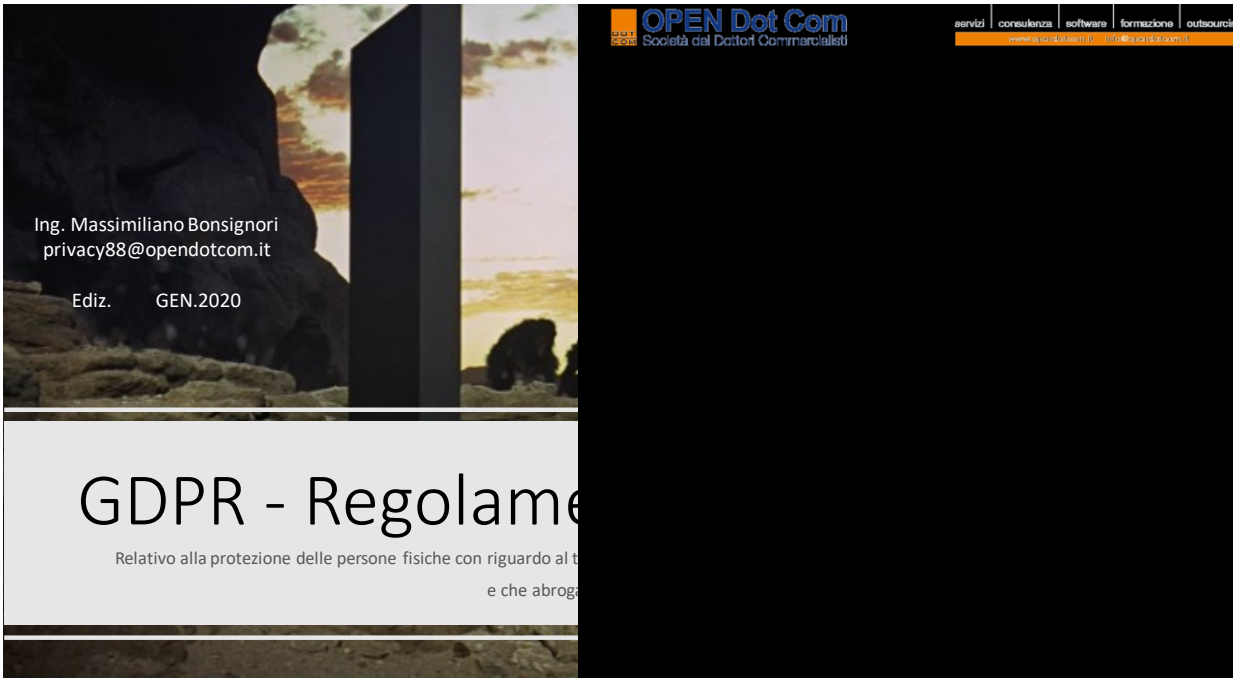
1

Prima di cominciare, un breve sondaggio…

grazie per la collaborazione

https://forms.gle/AZuUKcjMT8st74pP6

2


Ing. Massimiliano Bonsignori
privacy88@opendotcom.it
Ediz. GEN.2020
GDPR - Regolame
Relativo alla protezione delle persone fisiche con riguardo al t
e che abroga
OPEN Dot Com
Società dei Dottori Commercialisti
servizi
consulenza
software
formazione
outsourci

3


Dal 25/05/2018
le nuove norme
sono applicabili
in tutta la UE
…e prevalgono sulle normative nazionali, adeguate alle previsioni del nuovo regolamento che è già in vigore

5


Dal 19/09/2018
è in vigore il D.Lgs. 101/18
che adegua il Codice Privacy al
GDPR
Pertanto il D.Lgs. 196/2003, pesantemente modificato continua ad esistere!

6

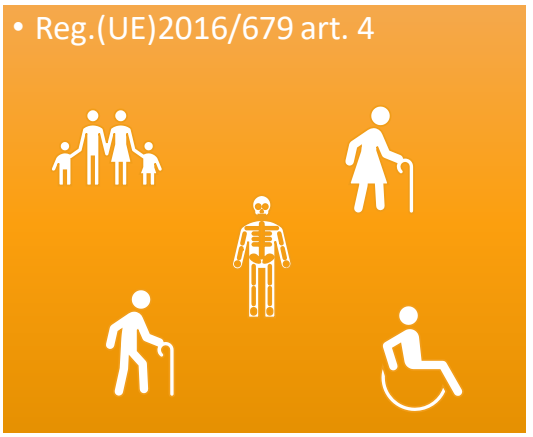

GDPR
General Data Protection Regulation

7

8

Dato personale

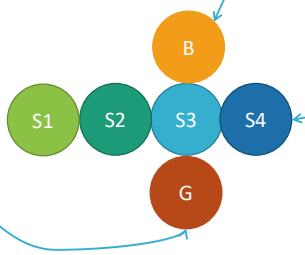
- qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);



9

Categorie particolari di dati personali

- (G) Dati genetici
- (B) Dati biometrici (identificativi)



- Dati Sensibili (ex D.Lgs 196/03)
- Si tratta di dati personali "umani" idonei a rivelare:
- (S1) l'origine razziale ed etnica
- (S2) le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- (S3) lo stato di salute
- (S4) la vita sessuale

10

Dati relativi a condanne penali e reati o a connesse misure di sicurezza

d.lgs.196/2003 art. 4
dati personali giudiziari

- i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale

Reg.(UE)2016/679 art. 10

- Dati relativi a condanne penali e reati o a connesse misure di sicurezza

11

Dati anonimi

- Quei dati che in origine, o a seguito di trattamento, non possono essere in nessun modo associati ad un interessato identificato o identificabile.
- **Quindi non sono dati personali**

Dati pseudonimi

- Quei dati personali che non possono più essere attribuiti a un interessato specifico **senza l'utilizzo di informazioni aggiuntive**, conservate separatamente e soggette a misure tecniche e organizzative adeguate a garantire tale separazione

12

Tipi di trattamento

13

Trattamento

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

- Reg.(UE)2016/679 art. 4

14

Comunicazione

Diffusione

15

Profilazione

GPDP, Provvedimento n. 161 del 19 marzo 2015 [doc. web n. 3881513]

- analisi e elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente (cd. single out) ovvero del terminale e, per il suo tramite, anche del profilo, appunto, di uno o più utilizzatori di quel dispositivo

Reg.(UE)2016/679 art. 4

- 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

16

Es. Pubblicità comportamentale

Your Online Choices
a guide to online behavioural advertising

- http://www.youronlinechoices.com/it/le-tue-scelte
- http://www.youronlinechoices.com/it/

17

Pseudonimizzazione

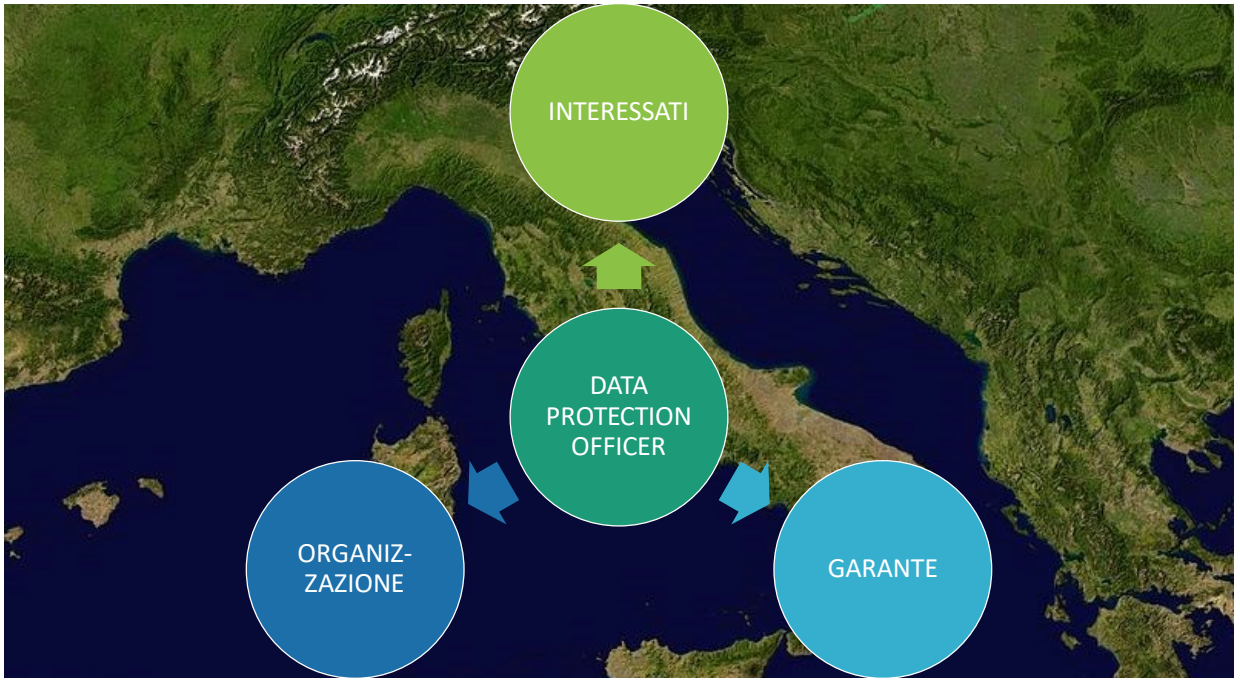
- il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese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

- Reg.(UE)2016/679 art. 4

18

Ruoli

19



20

Responsabile della protezione dei dati (RPD ovvero DPO=Data Protection Officer)

- la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo designato dal titolare o dal responsabile affinché sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

- Reg.(UE)2016/679 artt. 37-39

21

Titolare del trattamento (data controller)

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

- Reg.(UE)2016/679 art. 4

22

Contitolari del trattamento

- due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento

- Reg.(UE)2016/679 art. 26

23

Responsabile del trattamento (data processor)

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento
- se un responsabile del trattamento viola il regolamento, determinando le finalità e i mezzi del trattamento, va considerato titolare del trattamento in questione

- Reg.(UE)2016/679 art. 4, art. 28 co.10

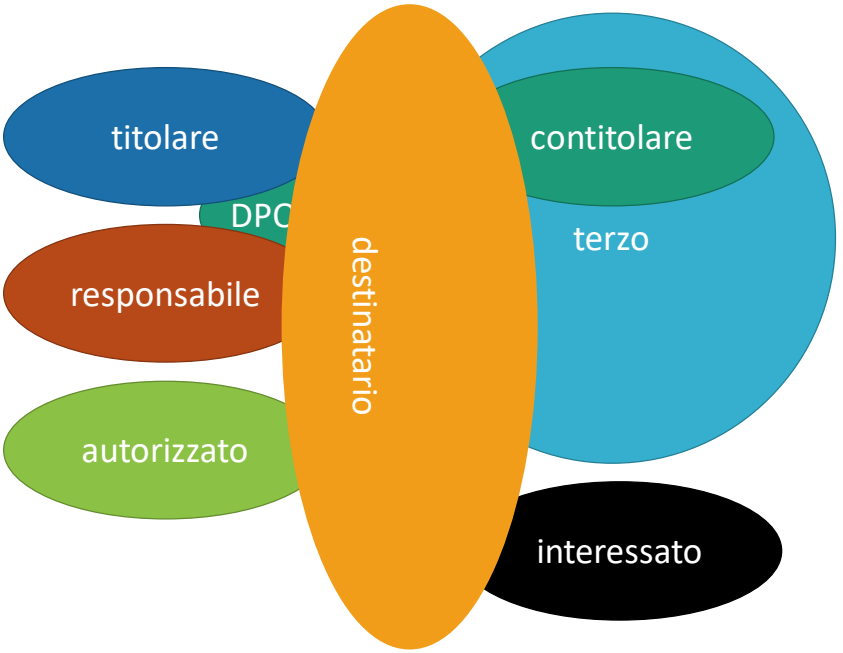
24

Autorizzati trattamento (persons authorized)

- le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

- Reg.(UE)2016/679 art. 4

25



26

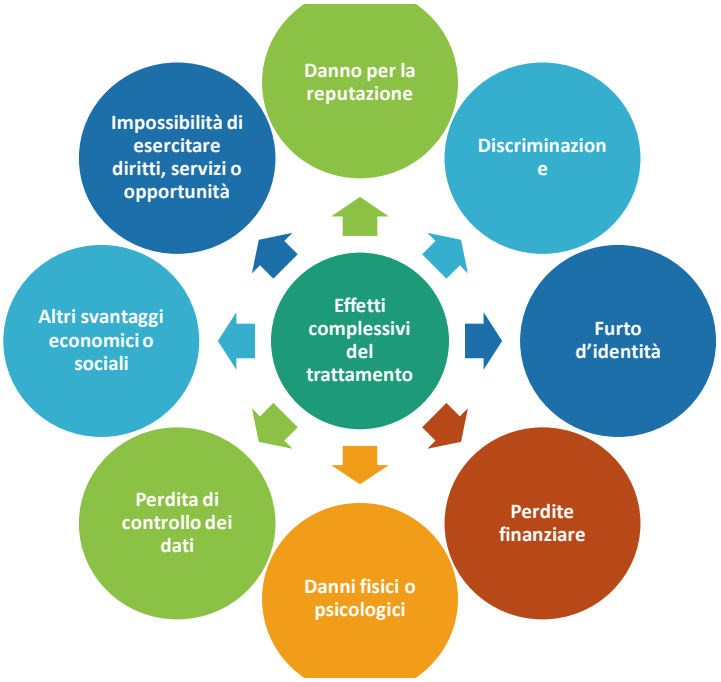
Principi applicabili & accountability

- Il titolare del trattamento deve essere in grado di comprovare il rispetto, che gli compete, di tutti i principi:

1. liceità, correttezza e trasparenza
2. limitazione della finalità
3. minimizzazione dei dati
4. esattezza
5. limitazione della conservazione
6. integrità e riservatezza

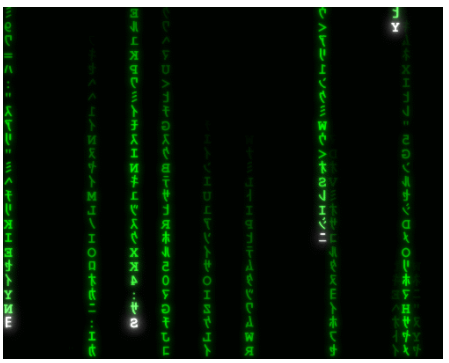
- Reg.(UE)2016/679 art. 5 co. 1 & 2

27



28

Diritti dell'interessato



29

Esistenza e Accesso

- 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
- L'interessato ha diritto di ottenere l'accesso ai dati personali e alle informazioni presenti nell'informativa

- Reg.(UE)2016/679 art. 16

- Es. le finalità del trattamento; le categorie di dati personali in questione; i destinatari; il periodo di conservazione; i diritti dell'interessato
- Es. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; l'esistenza di un processo decisionale automatizzato, compresa la profilazione, nonché l'importanza e le conseguenze previste

30

Copia dei dati

- L'interessato ha diritto di ottenere la comunicazione in forma intelligibile dei dati personali che lo riguardano

Reg.(UE)2016/679 art. 16

- Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.
  - In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

31

Rettifica

- L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
- Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa

- Reg.(UE)2016/679 art. 16

32

Cancellazione (diritto all'oblio)

- L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, se sussistono alcuni specifici motivi o ricorrono alcune condizioni.

- Reg.(UE)2016/679 art. 17

33

In caso di Limitazione di trattamento

- I dati personali possono essere trattati solo:

1. per la conservazione,
2. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
3. per tutelare i diritti di un'altra persona fisica o giuridica
4. per motivi di interesse pubblico rilevante
5. In tutti gli altri casi, soltanto con il consenso dell'interessato

- Reg.(UE)2016/679 art. 18

37

Portabilità

Reg.(UE)2016/679 art. 20

- qualora:

1. il trattamento si basi sul consenso o su un contratto **e**
2. il trattamento sia effettuato con mezzi automatizzati

- l'interessato deve poter migrare, senza impedimenti, i dati personali che lo riguardano da un titolare del trattamento a un altro titolare del trattamento
  - mediante un formato strutturato, di uso comune e leggibile da dispositivo automatico,
  - eventualmente mediante trasmissione diretta, se tecnicamente fattibile

39

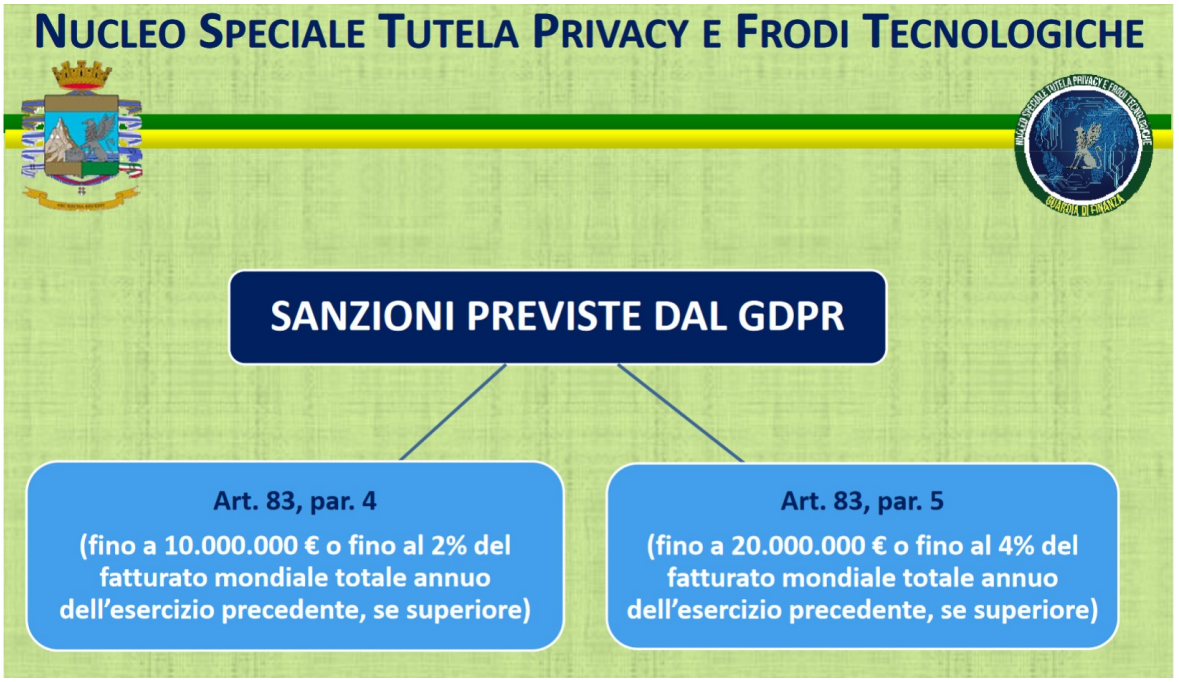
Opposizione

Reg.(UE)2016/679 art. 21

- L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano condotto sulla base di
  - Interesse pubblico o Esercizio di pubblici poteri
  - Legittimo interesse del titolare del trattamento
- Salvo che il titolare dimostri l'esistenza di motivi legittimi cogenti
  - per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure
  - per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

42

44



45

E' fissato solo il massimo

- 10 milioni di euro
- 2% dell'ultimo fatturato annuo

Adempimenti di titolare e responsabile

Misure di protezione

- 20 milioni di euro
- 4% dell'ultimo fatturato annuo

Trasferimenti verso paesi terzi

Provvedimenti correttivi dell'autorità di controllo

Acquisizione del consenso

Diritti e riscontro agli interessati

Principi di trattamento

Presupposti di legittimità

46

Violazioni (rif. enforcementtracker.com al 28/01/2020)	Numero	Somma	Media
Base giuridica insufficiente per l'elaborazione dei dati	67	€ 81.056.577,00	€ 1.209.799,66
Misure tecniche e organizzative insufficienti per garantire la sicurezza delle informazioni	43	€ 332.476.427,00	€ 7.732.009,93
Inosservanza dei principi generali di elaborazione dei dati	27	€ 16.067.874,00	€ 595.106,44
Adempimento insufficiente dei diritti degli interessati	20	€ 792.787,00	€ 39.639,35
Adempimento insufficiente degli obblighi di informazione	12	€ 550.765,00	€ 45.897,08
Cooperazione insufficiente con l'autorità di controllo	6	€ 18.511,00	€ 3.085,17
Adempimento insufficiente degli obblighi di notifica della violazione dei dati	5	€ 138.425,00	€ 27.685,00
Accordo sul trattamento dei dati insufficiente	2	€ 14.380,00	€ 7.190,00
Mancanza di nomina del responsabile della protezione dei dati	1	€ 10.000,00	€ 10.000,00
	Tot. 183		

47

individual fines (Top 10)

owing statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Country	Fine [€]	Type of Violation	Date
1	British Airways	UNITED KINGDOM	204,600,000	Insufficient technical and organisational measures to ensure information security	08 Jul 2019
2	Marriott International, Inc	UNITED KINGDOM	110,390,200	Insufficient technical and organisational measures to ensure information security	09 Jul 2019
3	Google Inc.	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
4	Austrian Post	AUSTRIA	18,000,000	Insufficient legal basis for data processing	23 Oct 2019
5	Deutsche Wohnen SE	GERMANY	14,500,000	Non-compliance with general data processing principles	30 Oct 2019
6	Telecoms provider (1&1 Telecom GmbH)	GERMANY	9,550,000	Insufficient technical and organisational measures to ensure information security	09 Dec 2019
7	Eni Gas e Luce	ITALY	8,500,000	Insufficient legal basis for data processing	11 Dec 2019
8	Eni Gas e Luce	ITALY	3,000,000	Insufficient legal basis for data processing	11 Dec 2019
9	National Revenue Agency	BULGARIA	2,600,000	Insufficient technical and organisational measures to ensure information security	28 Aug 2019
10	UWV (Dutch employee insurance service provider)	THE NETHERLANDS	900,000	Insufficient technical and organisational measures to ensure information security	31 Oct 2019

48

Illeciti Penali

d.lgs.196/2003

Art.	Tipologia	Sanzione
167 co.1	Trattamento Illecito dei dati – e-privacy	Reclusione 6-18 mesi
167 co.2	Trattamento Illecito dei dati – dati particolari o relativi a condanne	Reclusione 12-36 mesi
167 co.3	Trattamento Illecito dei dati – trasferimenti extra-UE	Reclusione 12-36 mesi
167-bis	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala	Reclusione 12-72 mesi
167-ter	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Reclusione 12-48 mesi
168 co.1	Falsità in dichiarazioni al Garante	Reclusione 6-36 mesi
168 co.2	Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante	Reclusione 0-12 mesi
170	Inosservanza di provvedimenti del Garante	Reclusione 3-24 mesi

49

50

Adempimenti vs. garante

COMUNICAZIONE DEI DATI DEL DPO

NOTIFICAZIONE IN CASO DI DATA BREACH

CONSULTAZIONE PRELIMINARE

RISPOSTA ALLE RICHIESTE E LEALE COLLABORAZIONE

51

Adempimenti vs. interessati

Rendere informativa

Gestire eventuale consenso/opposizione (OPT-IN vs. OPT-OUT)

Rispondere alle richieste di esercizio dei diritti

Effettuare le comunicazioni necessarie/opportune in caso di data breach

52

Adempimenti organizzativi (1)

autorizzazioni al trattamento

designazioni dei responsabili del trattamento e/o contitolari con eventuali trasferimenti extra ue

registri delle attività di trattamento (reat)

valutazione di impatto (dpia)

53

Adempimenti organizzativi (2)

Procedure di privacy by-design/default,

Misure di sicurezza

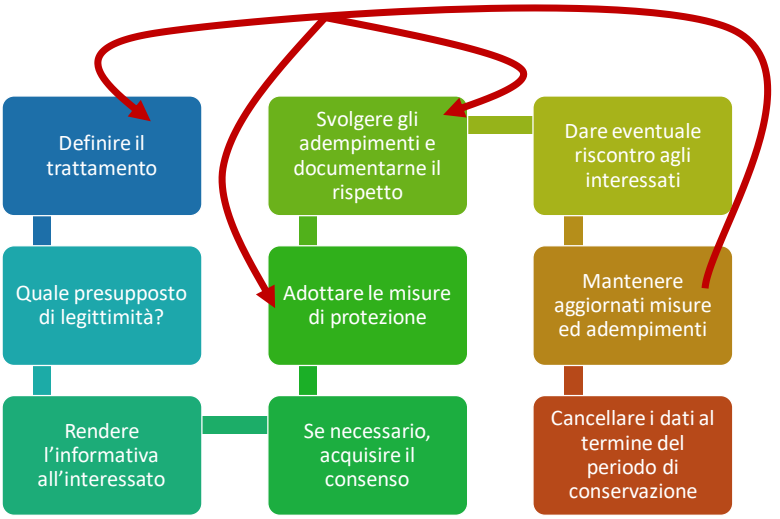
procedure per gestire gli altri adempimenti (es. vs. interessati/garante, cancellazione/conservazione dei dati)

Certificazioni e codici di condotta

54

Il «gioco» della privacy

.. una metafora applicativa



55

Quale presupposto di legittimità?

Liceità del trattamento

56

Divieto di trattare le categorie particolari di dati personali (sensibili, genetici, biometrici)

57

Trasferimenti di dati verso paesi terzi o organizzazioni internazionale

- Il trasferimento verso un paese terzo o un'organizzazione internazionale di dati personali destinati a essere oggetto di un trattamento dopo il trasferimento può avere luogo

1. sulla base di una decisione di adeguatezza della Commissione UE
2. se sussistono garanzie adeguate quali, tra l'altro,
   a) Norme vincolanti d'impresa
   b) Clausole contrattuali tipo

https://www.cnil.fr/en/data-protection-around-the-world

- Reg.(UE)2016/679 art. 44

58

Privacy by design

Reg.(UE)2016/679 art. 25

fin dalla progettazione,

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte a

1. attuare in modo efficace i principi di protezione dei dati (es. Minimizzazione)
2. a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

   - 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

59

Privacy by default

Reg.(UE)2016/679 art. 25

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire

1. 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
2. che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

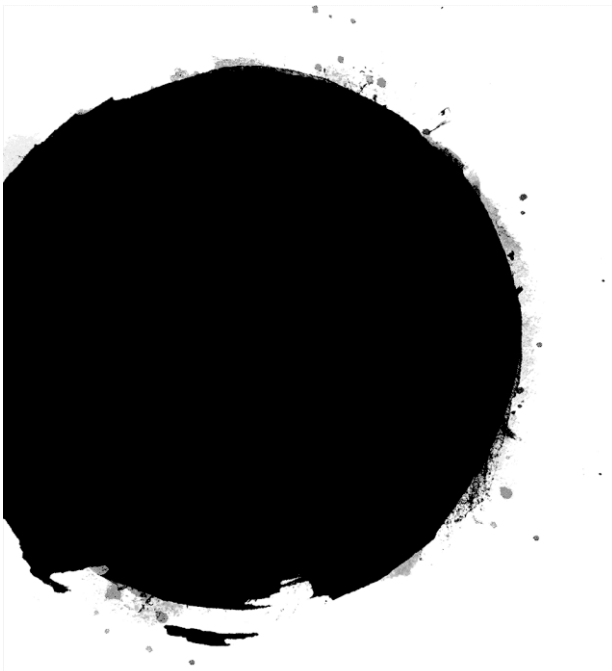
60

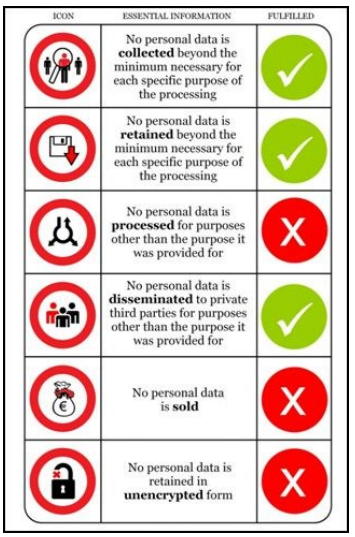
Rendere l'informativa all'interessato

Informativa

non si applica se e nella misura in cui l'interessato dispone già di tutte le informazioni previste

61





62

Misure di sicurezza

Reg.(UE)2016/679 art. 32

- Pseudonimizzazione
- Cifratura dei dati personali
- Capacità di assicurare su base permanente **la riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento
- Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

63

QUALI SONO LE MISURE PER LA GESTIONE DEL RISCHIO? ACCOUNTABILITY

64

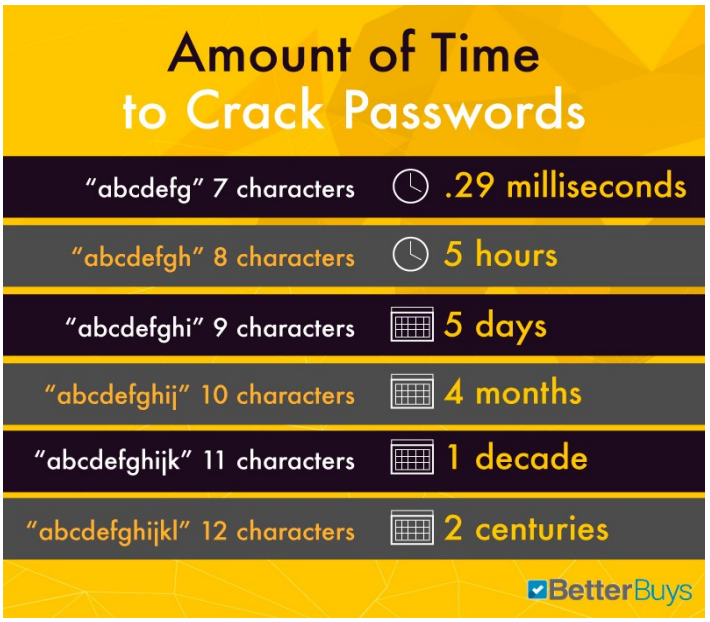
Misure di sicurezza (2)

d.lgs.196/2003 artt. 33-36 Allegato B

Nel caso di utilizzo di strumentazione elettronica:

- Utilizzazione di un sistema autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- Adozione di procedure per la custodia di copie di sicurezza (back-up), il ripristino della disponibilità dei dati e dei sistemi
- Aggiornamento periodico di sistemi operativi, software di protezione e di trattamento

65



66

Password: buone prassi

- Scegliere una password lunga (almeno 8 caratteri);
- Renderla complessa, evitando parole presenti nel vocabolario o sequenze di numeri facili da individuare da parte di un umano o di un software;
- Inserire sempre un mix di numeri, lettere maiuscole e minuscole, eventualmente segni di punteggiatura;
- Usare password diverse per l'accesso a servizi diversi;
- Scegliere password che si possano ricordare
  - magari una “passphrase”, una frase facile da ricordare ma “complicata” da acronimi, numeri e maiuscole
- Cambiare periodicamente la password ogni 3 mesi per i dati «rilevanti» e ogni 6 mesi negli altri casi

67

Password: errori più comuni da evitare

- Usare una parte qualsiasi del proprio nome
- Il nome del proprio account, ovvero il cosiddetto UserID (identificativo utente).
- Una parola con meno di 7 caratteri
- Una parte qualsiasi del nome di un membro della propria famiglia (animali domestici inclusi) o, peggio, quello di un collega
- Nomi di sistemi operativi
- Numeri con significati particolari (ad esempio, numeri di telefono e targhe automobilistiche)
- Nomi di luoghi
- Cose preferite o più detestate
- Facili associazioni con cose preferite o detestate: per esempio, "Aragorn" è una password pessima per un fan de "Il Signore degli Anelli"
- Una qualsiasi parola dalla corretta grammatica, in inglese come nella propria lingua madre, specialmente quelle che con ogni probabilità sono incluse in dizionari di parole d'uso comune. Ad esempio, "il mio nome" è una password non idonea per chi parla italiano

68

GRUPPO DI MISURE ORGANIZZATIVE	CONTROLLI RILEVANTI rif. ISO/IEC 27001: 2013	
Politica di sicurezza e procedure per la protezione dei dati personali	A.5 Security policy	Poltica di sicurezza
Ruoli e responsabilità	A.6.1.1 Information security roles and responsibilities	Ruoli e responsabilità per la sicurezza delle informazioni
Politica di controllo degli accessi	A.9.1.1 Access control policy	Politica di controllo degli accessi
Gestione di risorse / asset	A.8 Asset management	Gestione degli asset
Gestione del cambiamento	A.12.1 Operational procedures and responsibilities	Procedure operative e responsabilità
Responsabili del trattamento	A.15 Supplier relationships	Relazioni con i fornitori
Gestione degli incidenti / Violazioni dei dati personali	A.16 Information security incident management	Gestione degli incidenti relativi alla sicurezza delle informazioni
Business continuity (Continuità operativa)	A.17 Information security aspects of business continuity management	Aspetti della gestione della continuità operativa relativi alla sicurezza delle informazioni
Riservatezza da parte del personale	A.7 Human resource security	Sicurezza delle risorse umane
Formazione	A.7.2.2 Information security awareness, education and training	Consapevolezza, formazione e addestramento per la sicurezza delle informazioni

69

GRUPPO DI MISURE TECNICHE	CONTROLLI RILEVANTI rif. ISO/IEC 27001: 2013	
Controllo degli accessi e autenticazione	A.9 Access control	Controllo deli accessi
Registrazione dei log e monitoraggio	A.12.4 Logging and monitoring	Registrazione dei log e monitoraggio
Sicurezza di server / database	A.12 Operations security	Sicurezza operativa
Sicurezza delle postazioni di lavoro	A.14.1 Security requirements of information systems	Requisiti di sicurezza dei sistemi informativi
Sicurezza di rete e delle comunicazioni	A.13 Communications Security	Sicurezza delle comunicazioni
Back-up (Salvataggi di sicurezza)	A.12.3 Back-Up	Back-up
Dispositivi mobili / portatili	A.6.2 Mobile devices and teleworking	Dispositivi mobili e telelavoro
Sicurezza nell'intero ciclo di vita dell'applicazione	A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	Gestione delle vulnerabilità tecniche & Sicurezza nei processi di sviluppo ed assistenza
Cancellazione/distruzione dei dati	A.8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	Smaltimento dei supporti & Smaltimento sicuro o riutilizzo delle attrezzature
Sicurezza fisica	A.11 – Physical and environmental security	Sicurezza fisica ed ambientale

70

Formazione e Istruzioni obbligatorie

Reg.(UE)2016/679
art. 29, art. 32 co.4

- Chiunque (incaricato o responsabile) abbia accesso ai dati deve essere istruito al riguardo da parte del titolare del trattamento

71

Contratto di responsabilità

Reg.(UE)2016/679
art. 28 co.3, 9

- è stipulato in forma scritta, anche in formato elettronico
- prevede, in particolare, alcuni obblighi per il responsabile del trattamento

72

L'organizzazione deve:

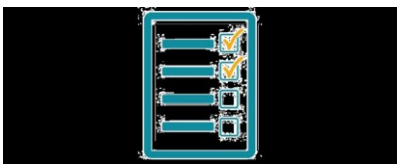
- Nominare i propri fornitori / collaboratori esterni
- Farsi nominare dai propri clienti nei casi previsti
  - cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970

73

Tenuta dei Registri delle attività di trattamento

Reg.(UE)2016/679 art. 30

- Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte.
- Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento



74

Valutazione di impatto (DPIA=Data Protection Impact Assessment)

Reg.(UE)2016/679 art. 35

il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

1. In generale, quando il trattamento può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento
2. In particolare, obbligatoria in taluni casi (…)
3. Salvo i casi in cui ciò non sia esplicitamente escluso (…)

75

Situazioni in cui vige l'obbligo della Valutazione di impatto

Reg.(UE)2016/679 art. 35 co.3/4

1. valutazione **sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche
2. trattamento, **su larga scala**, di categorie particolari di dati personali (sensibili, genetici, biometrici identificativi) o di dati relativi a condanne penali e a reati (giudiziari)
3. la sorveglianza sistematica **su larga scala** di una zona accessibile al pubblico.
4. per le tipologie di trattamenti inserite negli elenchi predisposti dalle autorità di controllo

77

Esempi di trattamenti su «larga scala»

trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati

trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività

trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio)

trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

sorveglianza svolta da un'impresa di sicurezza privata relativa a più centri commerciali e aree pubbliche

80

Documentazione in merito alla violazione dei dati personali

Reg.(UE)2016/679 art. 33

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese:

1. le circostanze a essa relative
   - natura, categorie e numero approssimativo di interessati
2. le conseguenze probabili
3. i provvedimenti adottati e da adottare per porvi rimedio
4. il rischio per i diritti e le libertà delle persone fisiche
   - su cui si basano i due successivi adempimenti

82

Hai subito un databreach dei tuoi dati?

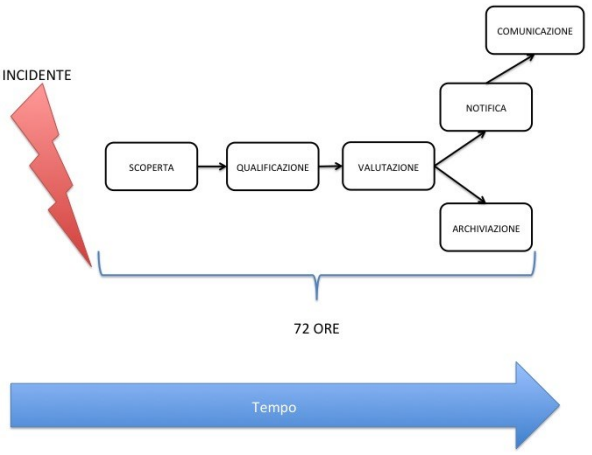
https://monitor.firefox.com/

83

Notifica di una violazione dei dati personali all'autorità di controllo

- In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente
  - senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza,
- a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

- Reg.(UE)2016/679 art. 33

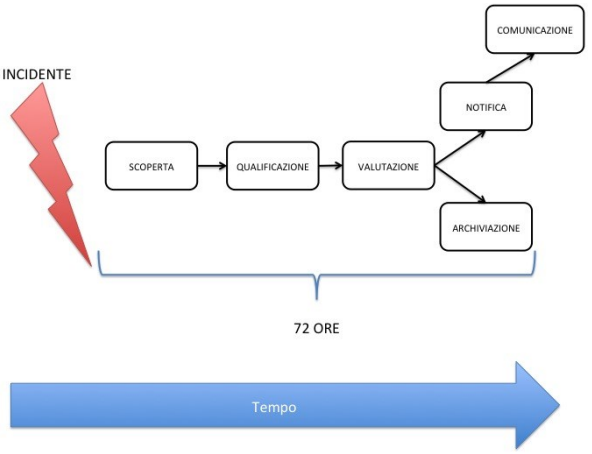


84

Comunicazione di una violazione dei dati personali all'interessato

- Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo
  - Salvo che i dati non fossero cifrati, ecc.

- Reg.(UE)2016/679 art. 34



85

Riesame ed aggiornamento

- Le misure

Reg.(UE)2016/679 art. 24

  - tecniche e organizzative
  - adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento
- sono riesaminate e aggiornate qualora necessario

Reg.(UE)2016/679 art. 35 co.11

- Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento

86

Conclusione del trattamento

Reg.(UE)2016/679 considerando 39

- Per assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica

- Alternativa alla cancellazione è l'Anonimizzazione. Infatti il GDPR non si applica al trattamento di tali informazioni anonime

87

Garanzia e Dimostrazione di conformità

Reg.(UE)2016/679 art. 24 co.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per

1. garantire ed
2. essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento.

- tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento,
- nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

88

Possibile dimostrazione di conformità

Reg.(UE)2016/679 art. 24 co. 

L'adesione a

- codice di condotta (articolo 40) o
- meccanismo di certificazione (articolo 42)

può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento

89