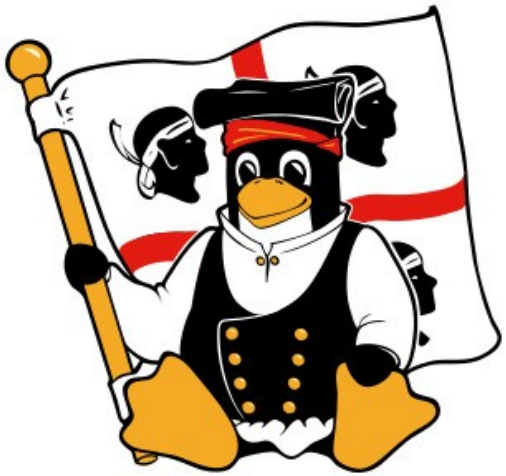
Avv. Giovanni Battista Gallus

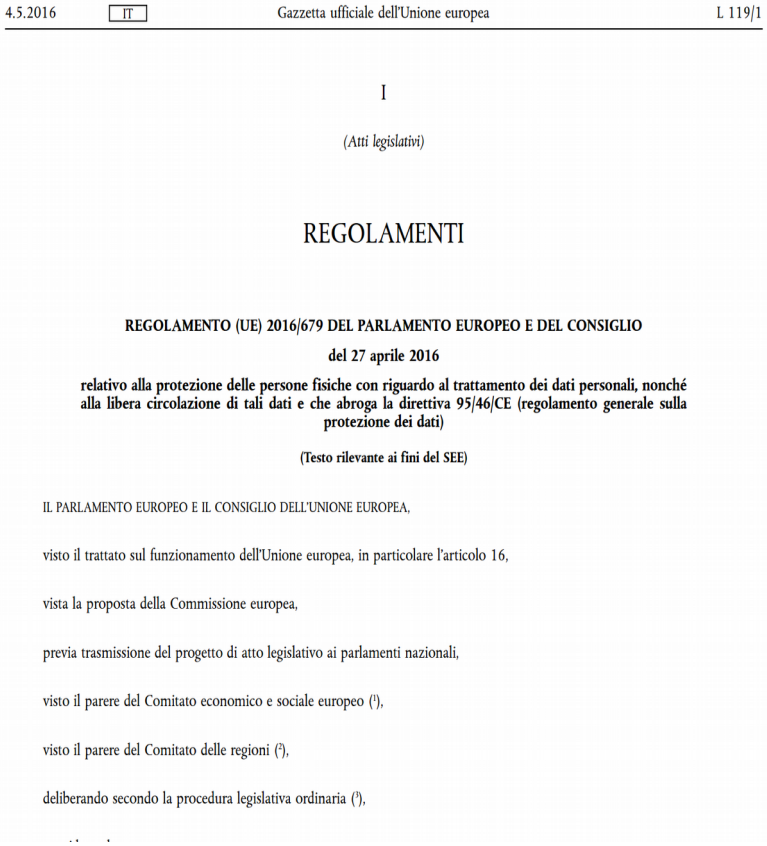
Prepararsi al Regolamento europeo sul trattamento dei dati personali (GDPR): il ruolo del free/open source software

Dipartimento di Informatica
Università di Cagliari
Palazzo delle Scienze
Via Ospedale, 72
Cagliari (CA)



25 maggio 2018
Una data memorabile

Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti



4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

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

visto il parere del Comitato delle regioni ([2]),

deliberando secondo la procedura legislativa ordinaria ([3]),

AMBITO DI APPLICAZIONE

PERSONE FISICHE

TRATTAMENTO DEI DATI PERSONALI

LIBERA CIRCOLAZIONE DEI DATI

Prepararsi al GDPR

FINALITA'	DETERMINATE	ESPLICITE	LEGITTIME
TRATTAMENTO	LECITO	CORRETTO	TRASPARENTE
DATI	ADEGUATI ESATTI AGGIORNATI	PERTINENTI	LIMITATI

Prepararsi al GDPR

Avv. Giovanni Battista Gallus @gbgallus

Avv. Paolo Lessio
CIRCOLOGIURISTITELEMATICI

Accountability

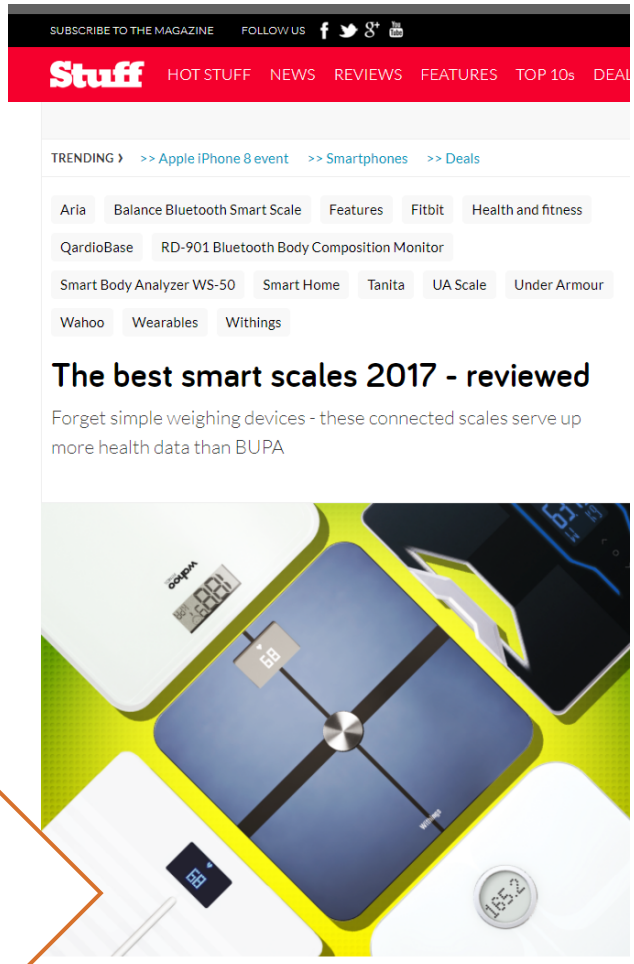
Dicesi accountability...

Prepararsi al GDPR

Sicurezza adeguata, "integrità e riservatezza"

F/LOSS IN IOT DEVICES

DATA PROTECTION BY DESIGN E BY DEFAULT



Prepararsi al GDPR

Responsabilizzazione

(DATA PROTECTION BY DEFAULT
E
DATA PROTECTION BY DESIGN)

i) Privacy by default: trattamento effettuato nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini;

ii) Privacy by design: incorporare la protezione dei dati personali sin dalla progettazione del flusso così da assicurare a) sicurezza durante tutto il ciclo del servizio; b) trasparenza; c) centralità dell'utente.

MISURE TECNICHE E ORGANIZZATIVE ADEGUATE

Avv. Paolo Lessio
CIRCOLOGIURISTITELEMATICI

Prepararsi al GDPR

REGISTRO ATTIVITA' DEL TRATTAMENTO

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzati- ve di cui all'articolo 32, paragrafo 1.

Avv. Paolo Lessio
CIRCOLOGIURISTITELEMATICI

SE:
Il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

Il trattamento integra una 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;

VALUTAZIONE DI IMPATTO DEL TRATTAMENTO SULLA PROTEZIONE DEI DATI PERSONALI

Prepararsi al GDPR

diritto di ricevere in un **formato strutturato, di uso comune e leggibile da dispositivo automatico** i dati personali che lo riguardano forniti a un titolare del trattamento e diritto di trasmettere tali dati a un altro titolare del trattamento **senza impedimenti da parte del titolare del trattamento cui li ha forniti**

Per i trattamenti

a) basati su consenso o contratto e

b) effettuati con mezzi automatizzati

Trasmissione diretta (se tecnicamente fattibile)

DATA PORTABILITY

OTTENERE L'INTEROPERABILITA' CON IL SOFTWARE LIBERO

DATA BREACH/AUTORITA'

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità di Controllo [… OMISSISS…] 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.

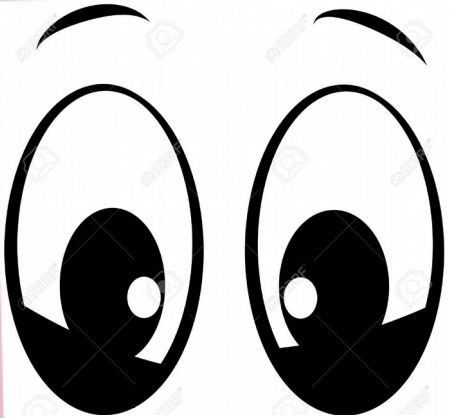
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) 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.

DATA BREACH/INTERESSATO

COMUNICAZIONE ELEMENTI:

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

Non è richiesta la comunicazione all'interessato se:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione (es. cifratura);
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.



DATA PROTECTION OFFICER

Avv. Paolo Lessio

CIRCOLOGIURISTITELEMATICI

Prepararsi al GDPR

La nomina del DPO
da parte del titolare
o del responsabile
(art. 37) è obbligatoria:

autorità pubblica
o organismo pubblico

Attività principali consistono
in trattamenti che,
per loro natura, ambito di applicazione
e/o finalità, richiedono il monitoraggio
regolare e sistematico degli interessati
su larga scala

Attività principali consistono
in trattamento , su larga scala,
di dati “particolari” e giudiziari

Prepararsi al GDPR

(art. 37)
I requisiti del DPO/RPD

Data Protection Officer
o
“Responsabile della protezione dei dati”

Conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati

Capacità di assolvere ai compiti

Indipendenza

Prepararsi al GDPR

La nomina del DPO
da parte del titolare
o del responsabile
(art. 37)

Obbligatoria
per autorità pubblica
o organismo pubblico

Può essere un dipendente
o un soggetto esterno

Può essere
un gruppo di lavoro

La nomina va pubblicata
e comunicata al Garante

Prepararsi al GDPR

Posizione del DPO
(art. 38)

Deve essere **tempestivamente** e **adeguatamente** coinvolto In tutte le questioni riguardanti la protezione dei dati personali

Non deve ricevere direttive per l'esecuzione dei compiti

Dotazione di risorse e formazione

Prepararsi al GDPR

Posizione del DPO
(art. 38)

- Divieto di rimozione o penalizzazione per adempimento dei compiti
- Riferisce direttamente ai vertici gerarchici
- Può essere contattato direttamente dagli interessati
- Attenzione al conflitto di interessi

Prepararsi al GDPR

Compiti del DPO
(art. 39)

- Informazione e consulenza sul trattamento di dati personali
- Controllo sull'osservanza del Regolamento e delle policy
- Cooperazione e punto di contatto con il Garante
- Consultazione in caso di valutazione d'impatto

SANZIONI
(art. 82 GDPR)

#brontobogasudinai

Violazione degli obblighi:
Sanzione amministrativa pecuniarie fino a 10 000 000 EUR,
o per le imprese, fino al 2 % del fatturato mondiale totale annuo

Violazione dei principi generali, dei diritti degli interessati etc:
Sanzione amministrativa pecuniarie fino a 20 000 000 EUR,
o per le imprese, fino al 4 % del fatturato mondiale totale annuo

Prepararsi al GDPR

Sophie Kwasny @SophieKwasny · 27 gen 2016

#CPDP2016 - **Privacin** pills - To use without moderation - not registered by @edqm_news :)

Traduci dalla lingua originale: inglese

6 8

Domande

Prepararsi al GDPR

Avv. Giovanni Battista Gallus @gbgallus

Grazie!

Avv. Giovanni Battista Gallus

gallus@array.eu @gbgallus