La privacy nello studio legale alla luce del GDPR e del D.Lgs. 101/2018
Treviso 14 dicembre 2018

P come Privacy

Avv. Nicola Gargano

ORDINE DEGLI AVVOCATI
BARI


Consultazione preventiva
Consultazione preventiva
Privacy Impact Assessment
Data Protection Officer
Accountability
Data Protection Officer
Accountability
Data Protection Officer
privacy by default
privacy by default
Data Breach
Data Protection Officer
Privacy Impact Assessment
Valutazione d'impatto sulla protezione dei dati
Accountability
Diritto Portabilità
privacy by default
Privacy Impact Assessment
Data Protection Officer
Consultazione preventiva
Accountability
Data Breach
Consultazione preventiva
Data Breach
Valutazione d'impatto sulla protezione dei dati
Diritto Portabilità
Registri delle attività di trattamento
Valutazione d'impatto sulla protezione dei dati
Accountability
Data Protection Officer
Data Breach
privacy by default
Valutazione d'impatto sulla protezione dei dati
Diritto Portabilità
privacy by design
Privacy Impact Assessment
privacy by design
Registri delle attività di trattamento
Diritto Portabilità
Data Breach
Data Breach
privacy by design
privacy by design
Data Breach
Accountability
Data Breach
Accountability
Diritto Portabilità
Diritto Portabilità
privacy by default
privacy by design
privacy by design
Accountability
Diritto Portabilità
Consultazione preventiva
Valutazione d'impatto sulla protezione dei dati
Registri delle attività di trattamento
Diritto Portabilità
Data Protection Officer
privacy by default
Privacy Impact Assessment
privacy by design
Registri delle attività di trattamento
Data Protection Officer
Consultazione preventiva
privacy by design

Tra vecchie e nuove norme

- **Decreto legislativo 30 giugno 2003, n. 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

https://www.youtube.com/watch?v=azb1VsXOpdw

DECRETO LEGISLATIVO 10 agosto 2018, n. 101 - (GU Serie Generale n.205 del 04-09-2018) Entrata in vigore del provvedimento: 19/09/2018

ERI ADEGUATO ?

- **Regolamento Europeo n.679/2016 - Regolamento europeo dei dati personali (GDPR)**

Applicazione diretta dal 25 maggio 2018

Proroghe?

art. 22 comma 13 del decreto legsilativo 10 agosto 2018 n. 101

13. Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie.

Altre fonti:

- LINEE GUIDA GRUPPO ART 29 WP29
- Codici di condotta

in attesa di verifica del garante per 90 gg	restano in vigore per 6 mesi (associazioni e altri organismi rappresentanti le categorie interessate sottopongano nuovi codici al garante)
A.1 CODICE DI DEONTOLOGIA RELATIVO AL TRATTAMENTO DEI DATI PERSONALI NELL'ESERCIZIO DELL'ATTIVITA' GIORNALISTICA. A.2 CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER IL TRATTAMENTO DI DATI PERSONALI PER SCOPI STORICI. A.3 CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI A SCOPI STATISTICI E DI RICERCA SCIENTIFICA EFFETTUATI NELL'AMBITO DEL SISTEMA STATISTICO NAZIONALE. A.4 come sopra ma solo STATISTICI E SCIENTIFICI A.6 Per il trattamento di dati personali per investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria	A.5. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti A.7 Informazione commerciale

- Autorizzazioni generali

Le autorizzazioni generali ?

Art. 21 Decreto legislativo

1. Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da porre in consultazione pubblica **entro novanta giorni dalla data di entrata in vigore del presente decreto**, **individua le prescrizioni contenute nelle autorizzazioni generali gia' adottate, relative alle situazioni di trattamento** di cui agli articoli 6, paragrafo 1, lettere c) ed e) (Obbligo legale o interesse pubblico), 9, paragrafo 2, lettera b) e 4, nonche' al Capo IX del regolamento (UE) 2016/679, **che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma e' adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.**
2. Le autorizzazioni generali sottoposte a verifica a norma del comma 1 che sono state ritenute **incompatibili con le disposizioni del Regolamento (UE) 2016/679 cessano di produrre effetti dal momento della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana del provvedimento di cui al comma 1.**
3. Le autorizzazioni generali del Garante per la protezione dei dati personali adottate prima della data **di entrata in vigore del presente decreto e relative a trattamenti diversi da quelli indicati al comma 1 cessano di produrre effetti alla predetta data.**
4. Sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 producono effetti, per la corrispondente categoria di dati e di trattamenti, le autorizzazioni generali di cui al comma 2 e le pertinenti prescrizioni individuate con il provvedimento di cui al comma 1.
5. Salvo che il fatto costituisca reato, le violazioni delle prescrizioni contenute nelle autorizzazioni generali di cui al presente articolo e nel provvedimento generale di cui al comma 1 sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento (UE) 2016/679.

I soggetti e l'ambito di applicazione

CHI SONO I TUTELATI ?

Interessato: persona fisica e non giuridica

E SU QUALI TRATTAMENTI ?

E CHI E' OBBBLIGATO A TUTELARLI ?

TRATTAMENTO INTERAMENTE AUTOMATIZZATO

TITOLARE DEL TRATTAMENTO

TRATTAMENTO PARZIALMENTE AUTOMATIZZATO

RESPONSABILE DEL TRATTAMENTO

AUTORIZZATI AL TRATTAMENTO

TRATTAMENTO NON AUTOMATIZZATO(archivi)

RESPONSABILE DELLA SICUREZZA DEI DATI (cd. DPO Data Protection Officer)

TRATTAMENTO EFFETTUATO IN UNIONE EUROPEA MA MATERIALMENTE COMPIUTO EXTRA UE o TRATTAMENTO NON COMPIUTO NELL'UE, MA CHE EFFETTUI PROFILAZIONE O OFFERTA DI BENI E SERVIZI A SOGGETTI CHE SI TROVANO NELL'UE

Le definizioni del regolamento

Titolare del trattamento = "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".

Responsabile del trattamento = "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento«.

Interessato = 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".

Dati personali = "qualsiasi informazione riguardante una persona fisica identificata o identificabile".

L'INCARICATO

Definito dal regolamento quale «Terzo» (c.26) soggetti identificati come "persone autorizzate al trattamento"; non sono definiti formalmente, ma disciplinati indirettamente anche in relazione all'obbligo, per il titolare, di indicarli espressamente.

La definizione del regolamento:

«**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

- **In linea di principio valgono le nomine conferite sotto la vigenza della Legge nazionale ma è necessario assicurarne la formazione**
- **I nuovi assunti (dopo il 28/5/2018) dovranno invece essere incaricati formalmente**

Articolo 28 - Responsabile del trattamento

1. **Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.**

2. **Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.**

Articolo 28 - Responsabile del trattamento

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il Titolare del trattamento

Non ha qualifica e specializzazioni particolari
Suo compito è di attuare misure tecniche ed organizzative adeguate a garantire (e quando serve anche a dimostrare) che il trattamento è effettuato conformemente al Regolamento.

Per realizzarlo può agire in autonomia ma anche aderire a codici di condotta o meccanismi di certificazione (ove esistenti o introdotti dalla Legge statale in conformità al Regolamento stesso).

Deve garantire il periodico riesame delle misure attuate ed il loro eventuale aggiornamento (se necessario).

IL TRATTAMENTO PUO' ESSERE ESERCITATO IN REGIME DI CONTITOLARITA'

In questo caso necessario un accordo interno che disciplini in modo trasparente le rispettive responsabilità, specifichi i ruoli di ogni titolare e i rapporti tra essi e gli interessati che, a loro volta devono essere informati di tutto ciò


Consultazione preventiva
Consultazione preventiva
Privacy Impact Assessment
Data Protection Officer
Accountability
Data Protection Officer
Accountability
Data Protection Officer
privacy by default
privacy by default
Data Breach
Data Protection Officer
Privacy Impact Assessment
Valutazione d'impatto sulla protezione dei dati
Accountability
Diritto Portabilità
privacy by default
Privacy Impact Assessment
Data Protection Officer
Consultazione preventiva
Accountability
Data Breach
Consultazione preventiva
Data Breach
Valutazione d'impatto sulla protezione dei dati
Diritto Portabilità
Registri delle attività di trattamento
Valutazione d'impatto sulla protezione dei dati
Accountability
Data Protection Officer
Data Breach
privacy by default
Valutazione d'impatto sulla protezione dei dati
Diritto Portabilità
privacy by design
Privacy Impact Assessment
privacy by design
Registri delle attività di trattamento
Diritto Portabilità
Data Breach
Data Breach
privacy by design
privacy by design
Data Breach
Accountability
Data Breach
Accountability
Diritto Portabilità
Diritto Portabilità
privacy by default
privacy by design
privacy by design
Accountability
Diritto Portabilità
Consultazione preventiva
Valutazione d'impatto sulla protezione dei dati
Registri delle attività di trattamento
Diritto Portabilità
Data Protection Officer
privacy by default
Privacy Impact Assessment
privacy by design
Registri delle attività di trattamento
Data Protection Officer
Consultazione preventiva
privacy by design

A come Accountability

Cosa cambia davvero?

Art. 5 GDPR "responsabilizzazione" (cd. accountability) ovvero adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento

Il vero obiettivo è diventare consapevoli

Autodeterminazione di: modalità, garanzie e limiti del trattamento dei dati, nel rispetto di disposizioni normative e regolamento (rendicontazione)

privacy by default **Art. 25 GDPR**

Rispetto dei principi generali di **pseudonimizzazione** e **minimizzazione**

privacy by design **Art. 25 GDPR**

protezione dei dati integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.

- Registri dell'attività del trattamento (art. 30)
- descrizione sommaria delle misure di sicurezza
- Finalità del trattamento
- Liceità del trattamento (Base giuridica, legge, contratto, consenso)

GDPR – Trattamenti leciti (Art. 6 – 7)

CONSENSO	ESECUZIONE DI UN CONTRATTO	ADEMPIMENTO DI OBBLIGO LEGALE
SALVAGUARDIA DI INTERESSI VITALI	ESECUZIONE DI UN COMPITO DI INTERESSE PUBBLICO	ESISTENZA DI LEGITTIMO INTERESSE DEL TITOLARE

GDPR – **Trattamento di categorie particolari di dati personali** (Art. 9) **Cd: dato sensibile**

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.

GDPR – **Trattamento di categorie particolari di dati personali** (Art. 9) **Cd: dato sensibile**

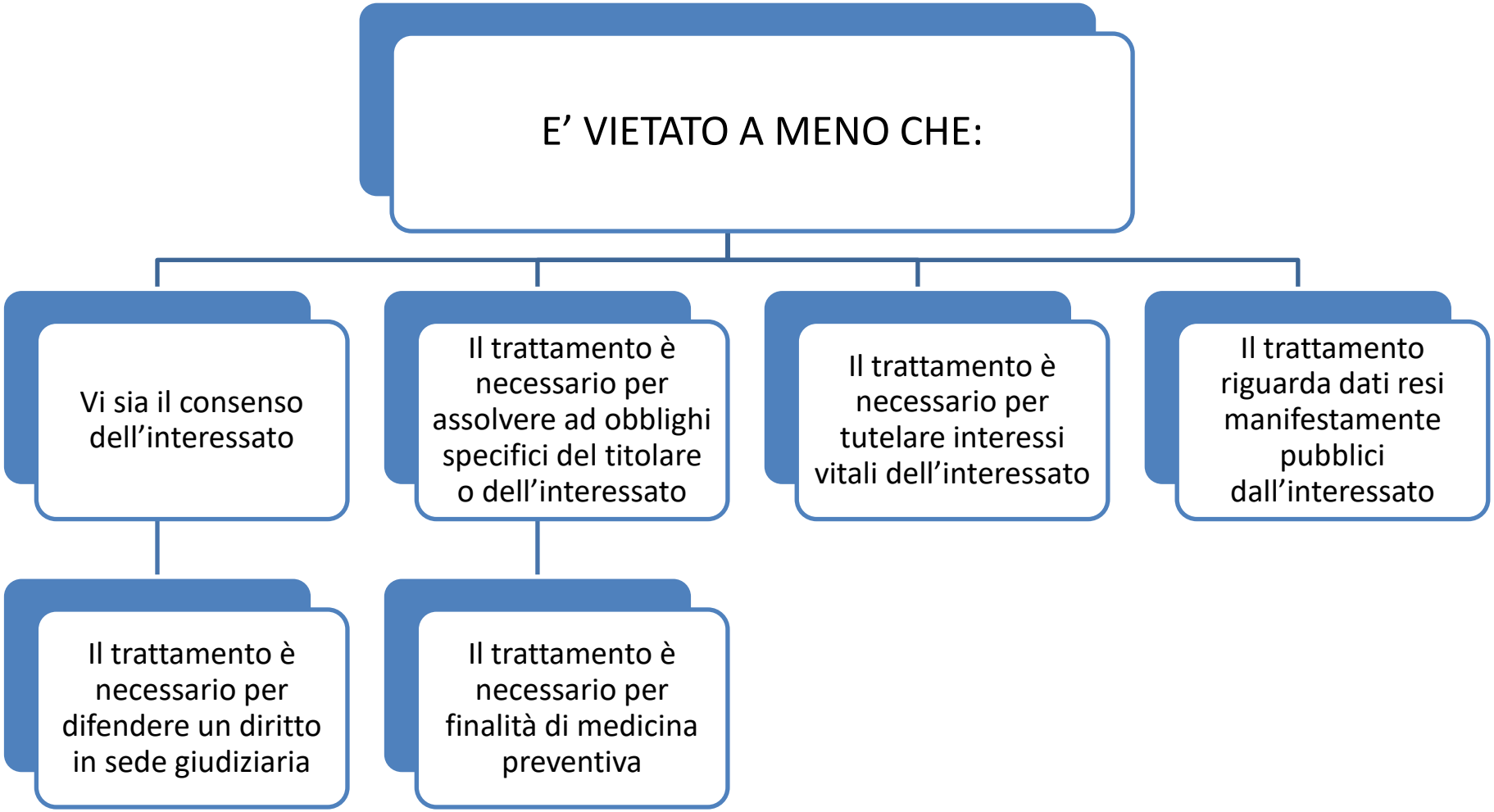
Alcune eccezioni:

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

Considerando52

La deroga dovrebbe anche consentire di trattare tali dati personali se necessario per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale

GDPR – **Trattamento di categorie particolari di dati personali** (Art. 9) **Cd: dato sensibile**



*Avv. **Raffaele Gargano***
Via Principe Amedeo, 190 – 70122 BARI
Via G. Compagnoni, 4 – 20129 MILANO
Tel. 080. 5213226/Fax 0805721169

Informativa ex art. 13 ai sensi del 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 (per brevità GDPR 2016/679)

1. **Titolare e responsabili del trattamento – art. 13 co. 1 lett. [a] [b] GDPR 2016/679**
   Titolare del trattamento è l'Avv. Raffaele Gargano con sede in con sede Via Principe Amedeo 190 Bari 70122, mail info@garganolex.it pec: raffaelegargano@legalmail.it
   al quale ci si potrà rivolgere per esercitare i diritti riconosciuti dal GDPR e per conoscere l'elenco aggiornato di tutti i Responsabili del trattamento dei dati.
2. **Finalità e base giuridica del trattamento – art. 13 co. 1 lett. [c] [d] GDPR 2016/679**
   I dati personali da Voi forniti saranno trattati unicamente per le seguenti finalità:
   - soddisfare le Vostre richieste in merito ai servizi che offriamo, e inviare comunicazioni di servizio;
   - eseguire le prestazioni da Voi richieste;
   - adempiere ad obblighi di legge;
   - ottemperare ad ordini provenienti da autorità;
   - esercitare e/o difendere un diritto nelle sedi competenti.

   Base giuridica dei suddetti trattamenti sono:
   - l'art. 6.1 [b] GDPR (necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso);
   - l'art. 6.1 [c] GDPR (necessità di adempiere un obbligo giuridico al quale è soggetto il titolare del trattamento;
   - per i dati particolari/sensibili, l'art. 9.2 [f] (necessità di accertare, esercitare o difendere un diritto in sede giudiziaria).

   I dati giudiziari – ossia quelli relativi alle condanne penali e ai reati ex art. 10 GDPR o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1 GDPR – vengono trattati nell'ambito della prestazione professionale con trattamento autorizzato dal diritto vigente con garanzie appropriate per i diritti e le libertà degli interessati.

   Non sono previsti ulteriori trattamenti basati sui legittimi interessi perseguiti dal titolare del trattamento.
3. **Tipi di dati trattati**
   Dati comuni - Dati particolari/sensibili - Dati giudiziari
4. **Comunicazione e diffusione dei dati – art. 13 co. 1 lett. [e] [f] GDPR 2016/679**
   I dati saranno comunicati solo all'interessato e a persone esplicitamente indicate dall'interessato, oppure per adempiere un obbligo giuridico al quale è soggetto il titolare del trattamento, oppure in quanto sia necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento. I dati saranno ulteriormente comunicati a soggetti terzi per finalità strettamente connesse all'esecuzione del mandato (ad es: domiciliatari, avvocati, collaboratori, consulenti, soggetti operanti nel settore giudiziario, controparti e relativi difensori, collegi di arbitri e, in genere, a tutti quei soggetti cui la comunicazione sia necessaria per il corretto adempimento delle finalità indicate nel punto 1) o per adempiere a obblighi di legge. I dati non saranno diffusi, né verranno trasferiti ad un paese terzo o a un'organizzazione internazionale. I dati comuni potranno altresì essere comunicati al commercialista del titolare (il cui nominativo potrà essere comunicato dal titolare su richiesta dell'interessato) per finalità contabili.

   Periodo di conservazione dei dati personali - art. 13 co. 2 lett. [a] GDPR 2016/679
   I dati saranno conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati conformemente a quanto previsto dagli obblighi di legge cui è sottoposto il titolare del trattamento.
5. **Diritti dell'interessato - art. 13 co. 2 lett. [b] [c] [d] GDPR 2016/679**
   L'interessato ha diritto di ottenere l'accesso ai dati personali e la loro rettifica.
   L'interessato, per motivi legittimi, ha diritto di ottenere la cancellazione degli stessi o la limitazione del trattamento dei dati che lo riguardano, o di opporsi al loro trattamento.
   L'interessato ha il diritto di proporre reclamo all'autorità di controllo – Garante per la protezione dei dati personali.
6. **Natura del conferimento dei dati personali e conseguenze di un eventuale rifiuto di rispondere - art. 13 co. 2 lett. [e] [f] GDPR 2016/679**
   Il conferimento dei dati personali è obbligatorio. L'eventuale rifiuto di conferirli comporta l'impossibilità di eseguire la prestazione professionale.
   Non esiste un processo decisionale automatizzato basato sui Suoi dati, né un trattamento che comporti la Sua profilazione.

Art. 13 GDPR Informativa anche con infografica

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.

Art. 13 GDPR Informativa (segue) dopo che sono stati ottenuti i dati personali:

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;

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;

Art. 13 GDPR Informativa (segue) dopo che sono stati ottenuti i dati personali:

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.

Importanza di definire gli obiettivi

IL CONSENSO

Considerando 32
Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Art. 35 GDPR valutazione d'impatto sulla protezione dei dati (c.d. privacy impact assessment)

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

a) 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

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; (dati giudiziari)

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

VIDEOSORVEGLIANZA E INFORMATIVA

La stai facendo male

Considerando 91 – Valutazione di impatto privacy – definizione di larga scala

- **trattamenti su larga scala**, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza.

- sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala.

Art. 30 GDPR registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

trattamento che possa presentare
un rischio per i diritti e le libertà dell'interessato,
trattamento non occasionale
trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (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.)

Art. 30 GDPR registro dei trattamenti

Cosa contiene il registro dei trattamenti:

a) nomi e contatti di: titolari e contitolari del trattamento, responsabili del trattamento e responsabile della protezione dei dati
b) le finalità del trattamento
c) descrizione delle categorie degli interessati e classificazione dei tipi di dati personali
d) categorie e destinatari oggetto di trasferimento dei dati trattati, sia nel territorio Paese ma anche a destinatari di paesi terzi o organizzazioni internazionali
e) le modalità e la documentazione delle garanzie per il trasferimento dei dati verso paesi terzi
f) i termini per la cancellazione delle categorie di dati
g) descrizione delle misure tecniche e organizzative

Art. 32 GDPR sicurezza del trattamento

….tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso….

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

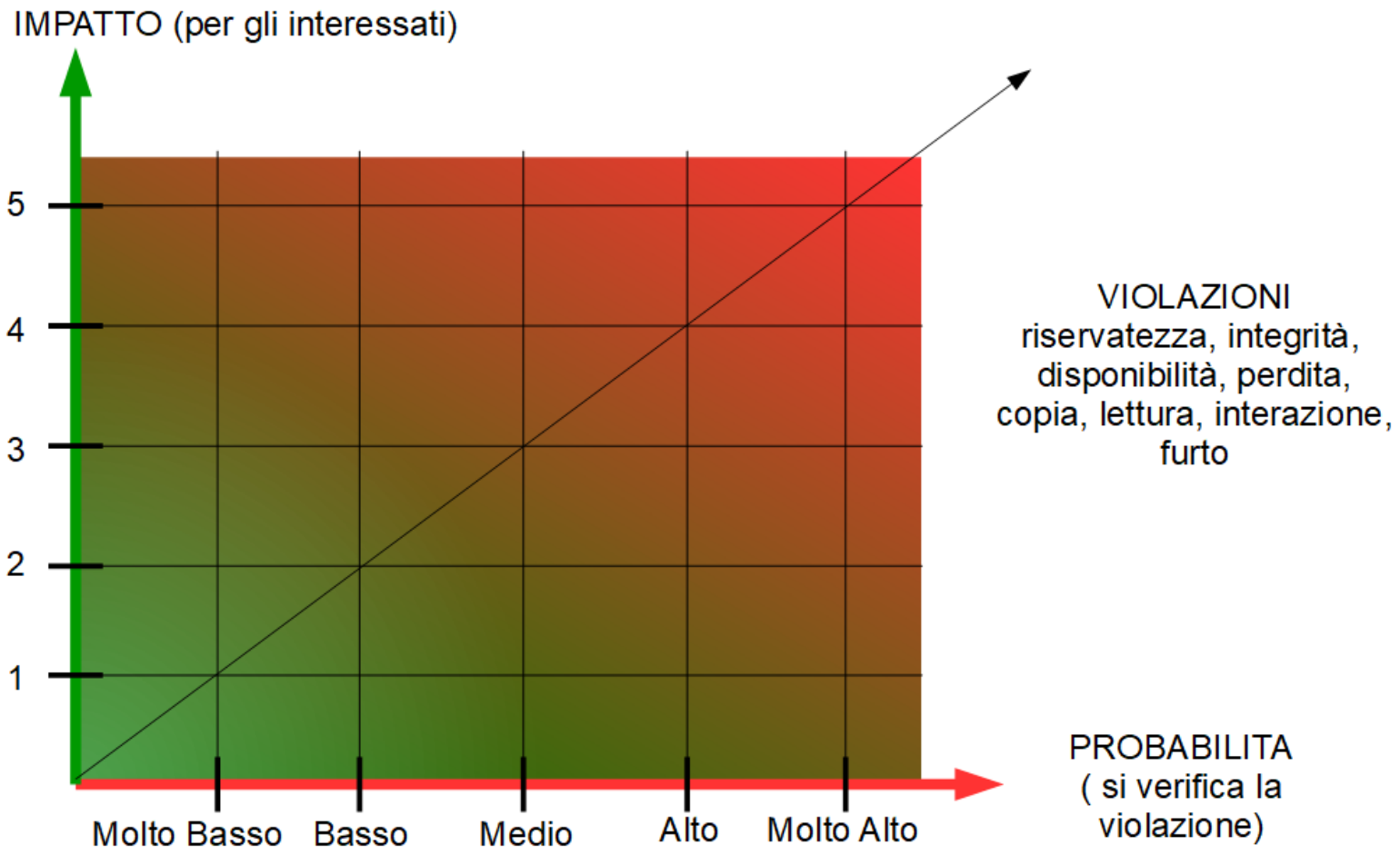
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 32 GDPR sicurezza del trattamento - le line guida del garante

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Rischi privacy: come valutarli.
Analisi di impatto per l'interessato e probabilità che si verifichi la violazioni



Graziano Albanese iCT – www.grazinaoalbanese.it


USB
HDD2
HDD1
LAN
STATUS
QNAP

D come Data Breach

Non credevo fosse un virus...
Piccola guida di sopravvivenza informatica per giuristi
MVLTA PAVCIS AG
GIUFFRÈ EDITORE

Il Data Breach

- Notificazione del data breach obbligo di notifica in capo al titolare del trattamento 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.

Al Garante art. 33 gdpr

"*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.".

All'interessato art. 34 gdpr *un rischio elevato per i diritti e le libertà delle persone fisiche*

- *Linguaggio semplice e chiaro*
- *Contenere le informazioni di cui alle lettere b), c) e d*

Il Data Breach

Il titolare è esentato dalla notifica all'interessato se:

- ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione (es. cifratura)

- ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati

- la comunicazione richiederebbe sforzi sproporzionati (in tal caso può effettuare una comunicazione unica pubblica).

S come Sanzioni

Sanzioni:

fino a 20.000.000 euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente

art.82 GDPR:

Diritto al risarcimento del danno (materiale o immateriale) causato da una violazione del Regolamento dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

Art. 166 codice da art. 167 a 168 sanzioni penali

SANZIONI

«**Art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).** - 1. Salvo che il fatto costituisca più grave reato, **chiunque**, al fine trarne **profitto per sé o altri ovvero di arrecare danno**, acquisisce con **mezzi fraudolenti** un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di **trattamento su larga scala** è punito con la reclusione da uno a quattro anni.
2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.»;

«**Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante).** - 1. Salvo che il fatto costituisca più grave reato, **chiunque**, **in un procedimento o nel corso di accertamenti dinanzi al Garante**, dichiara o attesta **falsamente** notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque **intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti**.»;

SANZIONI

«Art. 170 (Inosservanza di provvedimenti del Garante). - 1. Chiunque, **essendovi tenuto**, **non osserva** il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni.»;

«Art. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori). - 1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.»;

Il Data Protection Officer (DPO) “responsabile della protezione dati”

Responsabile della Protezione dei Dati (RPD)

Art. 37-38-39 GDPR

Considerando 97

«per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento.»

Scheda riassuntiva del garante:
http://194.242.234.211/documents/10160/0/Data+Protection+Officer+Scheda+informativa

FAQ SUL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) IN AMBITO PRIVATO

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

3. Chi sono i soggetti privati obbligati alla sua designazione?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

FAQ SUL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) IN AMBITO PRIVATO

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

- Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

FAQ SUL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) IN AMBITO PRIVATO

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

Trasferimento dati all'estero

Articolo 44

Principio generale per il trasferimento (C101, C102)

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

(102) Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati.

GDPR –Sicurezza del trattamento(Art. 32)

Misure tecniche organizzative adeguate (da valutare in relazione alla tipologia del trattamento *…se del caso..***)**

- Pseudonimizzazione
- Riservatezza, integrità e resilienza dei dispositivi e dei sistemi di trattamento
- Capacità di ripristino dei dati e loro accesso dapo un incidente tecnico o fisico (disaster recovery)
- Procedure di auditing periodiche delle misure tecniche e organizzative

Obiettivi e misure adeguate di sicurezza:

- Dispositivi (inventario dei dispositivi autorizzati)
- Software (inventario dei software autorizzati)
- Protezione delle configurazioni hardware e software (immagini e backup)
-Le vulnerabilità (valutazione e correzione continua)
- I privilegi di accesso a dispositivi e software
- Difese contro i malware
- Copie di sicurezza
-Protezione dei dati

Misure tecniche

Misure tecnologiche

- Firewall
- Sistemi per il monitoraggio dei dispositivi e dei software
- Difesa contro i malware
- Protezione dati
- Log e IPS (Intrusion prevention system)
- Server e sistemi da backup
- Protezione dei dati (crittografia)
- Protezione dei livelli di accesso
- Log degli accessi
- Procedure di disaster recovery (backup meglio se incrementale o differenziale)

PASSWORD

https://howsecureismypassword.net

Non credevo fosse un virus...
Piccola guida di sopravvivenza informatica per giuristi
MVLTA PAVCIS AG
GIUFFRÈ EDITORE

IL CLOUD COMPUTING

La gestione dei dati in cloud

QUALI CAUTELE?

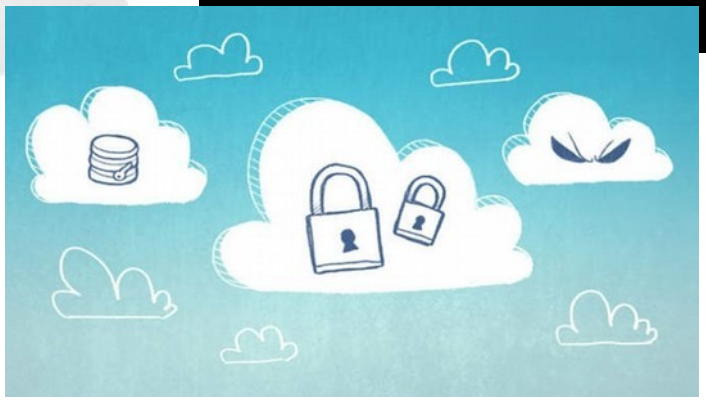
CCBE GUIDELINES ON THE USE OF CLOUD COMPUTING SERVICES BY LAWYERS

LINEE GUIDA DEL CCBE SULL'UTILIZZO DEI SERVIZI DI CLOUD COMPUTING DA PARTE DEGLI AVVOCATI

September 2012

Alcuni punti irrinunciabili (I)

Assicurare l'applicazione di sistemi di criptaggio dei file



Alcuni punti irrinunciabili (II)

Verificare che il fornitore dl servizio cloud non sia soggetto a una giurisdizione a longa manus che possa obbligarlo a condividere i dati degli avvocati europei memorizzati su server cloud con Authority nazionali non europee

Considerare di utilizzare provider di servizi cloud stabiliti all'interno della UE e non soggetti a longa manus di giurisdizione straniera

Prendere in considerazione procedure per la cifratura dei dati nella trasmissione e nell'archiviazione

Alcuni punti irrinunciabili (III)

Gli avvocati nella conclusione di un contratto di fornitura di servizi di cloud computing devono valutare:

[a] la solvibilità, affidabilità, proprietà ed adeguatezza patrimoniale del provider; [b] i potenziali rischi di conflitti di interesse; [c] i rischi di un eventuale uso improprio delle informazioni

[d] lo localizzazione esatta dei server di stoccaggio; [e] per quanto possibile, la sicurezza fisica ed elettronica dei server e del centro dati in cui sono ubicate; [f] le leggi civili, penali e costituzionali applicabili

Tratto da una storia vera

e-mail da uno studio legale:

"purtroppo ieri sera sono stati rubati i computer sia dell'avv. X che dell'avv. Y: chiediamo pertanto a tutti di rimandare le mail dell'anno 2015, compresa, se possibile, l'eventuale risposta. Grazie della collaborazione."

Grazie per l’attenzione

Avv. Nicola Gargano

nicgar@garganolex.it