GDPR

IL NUOVO REGOLAMENTO N. 679/2016 UE SULLA PROTEZIONE DEI DATI PERSONALI GUIDELINES, REGOLE, IMPATTI E SANZIONI

Avv. Stefano Orlandi
Esperto, Consulente ed autore di pubblicazioni
in materia di Data Protection

orlandi · leone & partners
STUDIOLEGALE

GDPR

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

Sommario

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)** (1) 1

orlandi · leone & partners
STUDIO LEGALE

CHE COSA C'E' DIETRO L'ANGOLO?

"*La direttiva europea di protezione dati è del 1995 ed è obsoleta*" **(Francesco Pizzetti, 2011)**
… non c'era Internet, **figuriamoci i Big data!**

orlandi · leone & partners
STUDIOLEGALE

CHE COSA C'E' DIETRO L'ANGOLO?

Il 25 gennaio 2012 la Commissione europea ha presentato ufficialmente le proposte relative al nuovo quadro giuridico europeo in materia di protezione dei dati. Si tratta di un Regolamento, che andrà a sostituire la direttiva 95/46/CE, e di una Direttiva che dovrà disciplinare i trattamenti per finalità di giustizia e di polizia (attualmente esclusi dal campo di applicazione della direttiva 95/46/CE).

A dicembre 2015 è stato approvato il testo definitivo.

Il nuovo Regolamento è stato pubblicato sulla GUUE L 119 del 4 maggio 2016.

orlandi · leone & partners
STUDIO LEGALE

TIMING

Articolo 99 Entrata in vigore e applicazione

Il presente regolamento **entra in vigore** il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea > **24 maggio 2016**

Esso **si applica** a decorrere dal **25 maggio 2018**

Il presente regolamento **è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.**

Art. 94 Abrogazione della direttiva 95/46/CE

La direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018

> fino ad allora si applicano le regole attuali.

orlandi · leone & partners
STUDIO LEGALE

CHE COSA C'E' DIETRO L'ANGOLO?

Gazzetta ufficiale dell'Unione europea

L 119

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

Sommario

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)** (1) 1

- right to rectification
- right to be forgotten
- right to erasure
- right to portability
- **ACCOUNTABILITY!**
- privacy by default
- privacy by design
- DPIA-data protection impact assessment
- DPO-data protection officer
- personal data breaches
- higher administrative fines (up to **20.000.000 EUR** or up to **4% of the total worlwide annual turnover**)

orlandi · leone & partners
STUDIOLEGALE

CAPO II PRINCIPI

Articolo 5
Principi applicabili al trattamento di dati personali

Liceità, correttezza e trasparenza = trattamento lecito, corretto e trasparente

Limitazione della finalità = raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità

Minimizzazione dei dati = adeguati, pertinenti e limitati a quanto necessario

Esattezza = esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti

Limitazione della conservazione = conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità

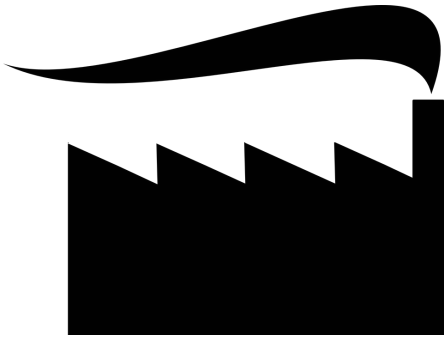
Integrità e riservatezza = trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

ACCOUNTABILITY

Il titolare del trattamento **è competente** per il rispetto dei principi e **in grado di comprovarlo**

RESPONSABILIZZAZIONE

CAPO IV TITOLARE E RESPONSABILE



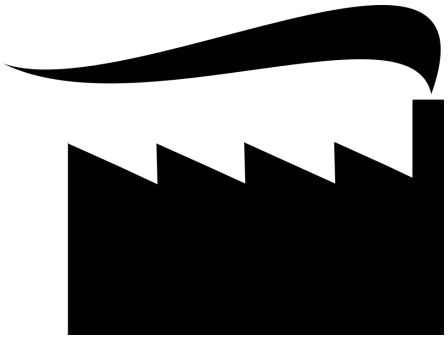
ACCOUNTABILITY

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**, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento

È opportuno stabilire la **responsabilità generale del titolare del trattamento** per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. **(considerando n. 74 GDPR)**

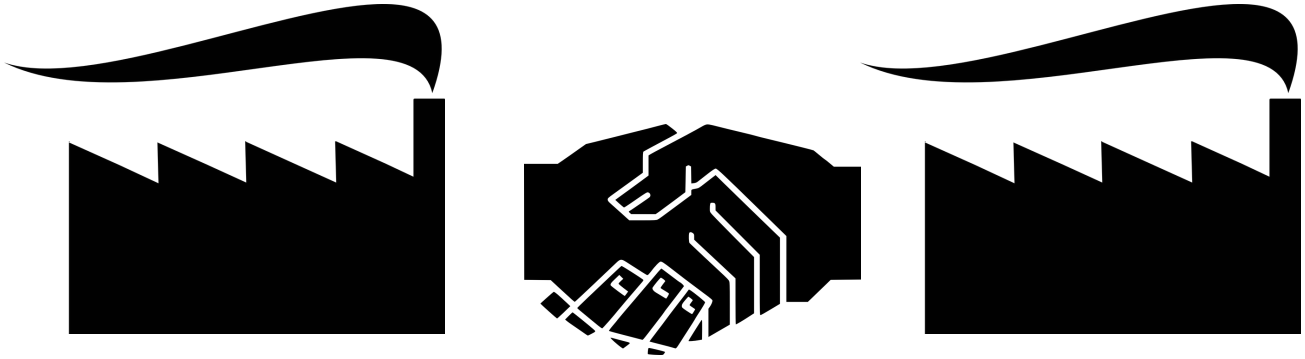
I SOGGETTI

CAPO IV TITOLARE E RESPONSABILE



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.

I SOGGETTI



Contitolari del trattamento

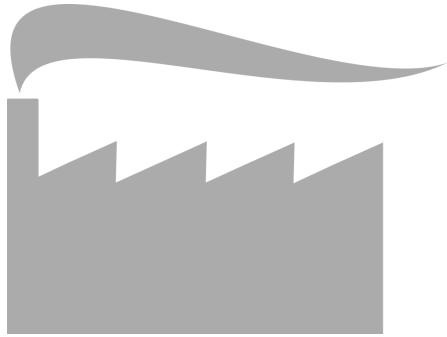
Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.Tale accordo può designare un punto di contatto per gli interessati.

L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento

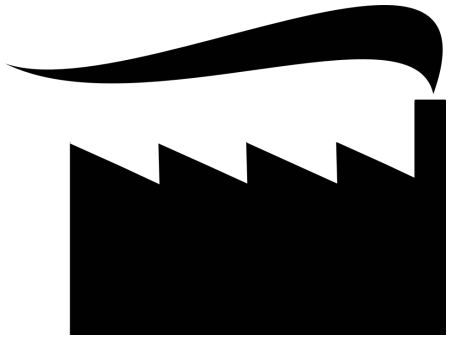
I SOGGETTI

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.



NB: se un responsabile del trattamento determina le finalità e i mezzi del trattamento dei dati in violazione del presente regolamento, è considerato un titolare del trattamento relativamente al trattamento in questione.

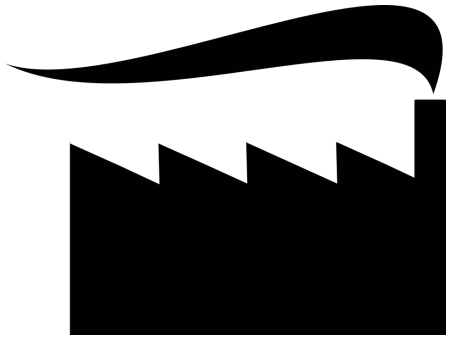
I SOGGETTI



CULPA IN ELIGENDO

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 ed organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

I SOGGETTI

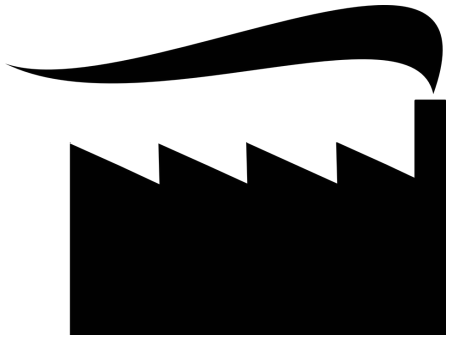


FORMA

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 contratto o altro atto giuridico è stipulato in **forma scritta, anche in formato elettronico.**

CAPO IV TITOLARE E RESPONSABILE



CONTENUTI MINIMI

materia disciplinata
durata del trattamento
natura e finalità del trattamento
tipo di dati personali
categorie di interessati
obblighi e diritti del responsabile del trattamento

I SOGGETTI

Il **contratto tra titolare e responsabile** deve prevedere che il responsabile:

a) tratti i dati personali **soltanto su istruzione documentata** del titolare del trattamento (…)

b) garantisca che l**e persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo statutario di riservatezza**;

c) adotti **tutte le misure (di sicurezza) richieste** ai sensi dell'articolo 32;

d) rispetti **le condizioni per ricorrere a un altro responsabile** del trattamento

e) **assista** il titolare del trattamento con misure tecniche ed organizzative adeguate al fine di soddisfare l'obbligo del titolare del trattamento di **dare seguito alle richieste per l'esercizio dei diritti dell'interessato**;

f) **assista** il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (**sicurezza; data breaches; DPIA; prior checking**), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

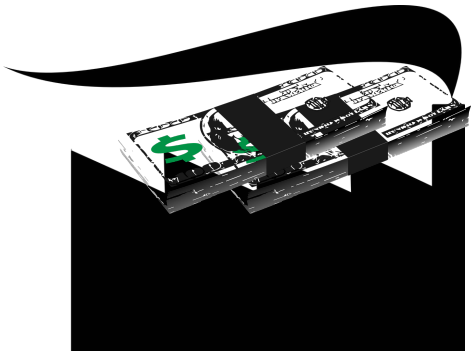
g) su scelta del titolare del trattamento, **cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione** dei servizi di trattamento di dati e cancelli le copie esistenti

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e **contribuisca agli audit, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato**.

Diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno **dal titolare del trattamento o dal responsabile del trattamento.**

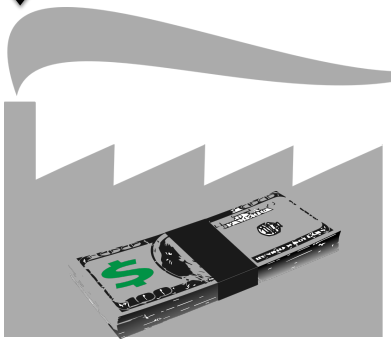
Ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.



Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al presente regolamento

"RECLAMO"
(rectius: "RIVALSA")

salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile.



Un responsabile del trattamento risponde per il danno cagionato dal trattamento **solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo esterno o contrario alle legittime istruzioni del titolare del trattamento.**

Il concetto di danno dovrebbe essere interpretato **in senso lato** alla luce della giurisprudenza della Corte di giustizia dell'Unione europea in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento **(considerando n. 146 GDPR)**

Sanzioni pecuniarie e altre sanzioni

ENTITA' DELLE SANZIONI PECUNIARIE
fino a **€ 10.000.000, o per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per violazione di

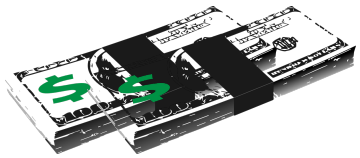
obblighi del titolare del trattamento e del responsabile del trattamento

8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
11 Trattamento che non richiede l'identificazione
25 Protezione dei dati fin dalla progettazione e protezione di default
26 Contitolari del trattamento
27 Rappresentanti di responsabili del trattamento non stabiliti nell'Unione
28 Responsabile del trattamento
29 Trattamento sotto l'autorità del titolare del trattamento e del responsabile del trattamento
30 Registri delle attività di trattamento
31 Cooperazione con l'autorità di controllo
32 Sicurezza del trattamento
33 Notificazione di una violazione dei dati personali all'autorità di controllo
34 Comunicazione di una violazione dei dati personali all'interessato
35 Valutazione d'impatto sulla protezione dei dati
36 Consultazione preventiva
37, 38, 39 Designazione (e posizione e compiti…) del responsabile della protezione dei dati

obblighi dell'organismo di certificazione
obblighi dell'organismo di controllo

Sanzioni pecuniarie e altre sanzioni

ENTITA' DELLE SANZIONI PECUNIARIE
fino a **€ 20.000.000, o per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per violazione di:



principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 (Principi applicabili al trattamento di dati personali; Liceità del trattamento; Condizioni per il consenso; Trattamento di categorie particolari di dati personali)

diritti degli interessati (artt. da 12 a 22)

trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO DEI DATI)

mancata osservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1

Pacchetto "*verso il GDPR*"

DURATA > fino al 30 APRILE 2018

CONTENUTI

1. formazione frontale per azzeramento su GDPR
2. sessioni di lavoro/webinar "live" da remoto
3. check up/audit GDPR, con report su azioni da effettuare
4. help desk privacy (email/tel/Skype) per tutto il periodo
5. mantenimento compliance Codice privacy e provv. connessi
6. newsletter, contenuti multimediali e aggiornamenti personalizzati

orlandi · leone & partners
STUDIO LEGALE

Pacchetto "*verso il GDPR+*"

DURATA > fino al 30 APRILE 2018

CONTENUTI

1. formazione frontale per azzeramento su GDPR
2. sessioni di lavoro/webinar "live" da remoto
3. check up/audit GDPR, con report su azioni da effettuare
4. help desk privacy (email/tel/Skype) per tutto il periodo
5. mantenimento compliance Codice privacy e provv. connessi
6. newsletter, contenuti multimediali e aggiornamenti personalizzati
7. **check up/audit su compliance Codice privacy e provv. connessi (Dlgs n. 196/2003)**
8. **adeguamento Codice privacy e provv. connessi**

orlandi · leone & partners
STUDIO LEGALE

Pacchetto "*GDPR*"

Disponibile da MAGGIO 2018 *(in corso di rifinitura)*

CONTENUTI

1. formazione frontale per azzeramento su GDPR
2. sessioni di lavoro/webinar "live" da remoto
3. **messa a norma GDPR**
4. help desk privacy (email/tel/Skype) per tutto il periodo
5. newsletter, contenuti multimediali e aggiornamenti personalizzati
6. **utilizzo gestionale "U2PIA" per compliance GDPR**
7. **repository documentale adempimenti privacy**

Il pacchetto "GDPR" sarà acquistabile **a condizioni di favore** da parte di tutte le FOB che avranno attivato, precedentemente, il pacchetto "verso il GDPR" o il pacchetto "verso il GDPR+".

orlandi · leone & partners
STUDIO LEGALE