

INQUADRAMENTO NORMATIVO

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

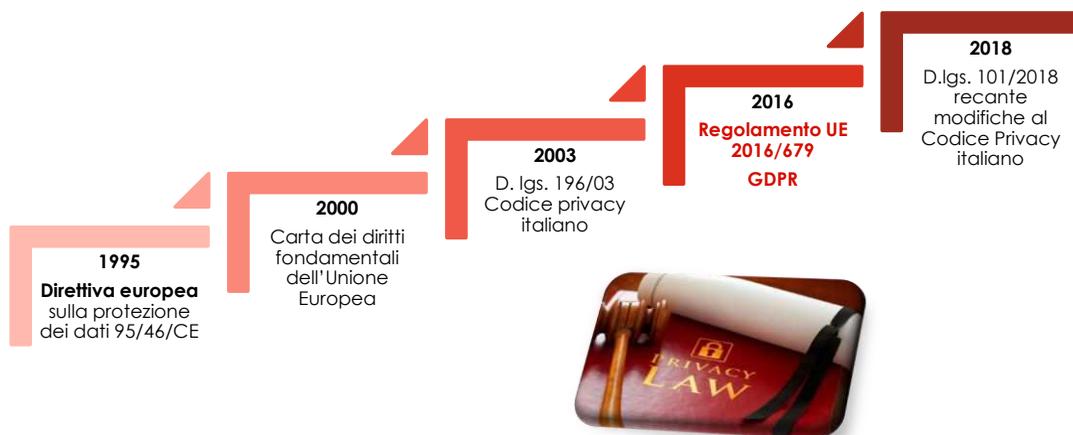
3

FONTI DEL DIRITTO

- **Regolamento UE 2016/679** «GDPR»;
- **Codice Privacy** D. lgs. 196/2003 e D. lgs. 101/2018;
- L. 300/1970 (**Statuto dei lavoratori**) e s.m.i. (v. Jobs Act);
- **Provvedimenti dell'Autorità Garante** per la protezione dei dati personali;
- **Pareri e linee guida WP29 / EDPB**, fra cui: Parere 08/2001 e Parere 02/2017 sul trattamento dei dati personali nel contesto lavorativo;
- **Codice dell'Amministrazione Digitale** d.lgs. 7 marzo 2005, n. 82;
- Determinazioni dell'**Agenzia per l'Italia Digitale** (AgID).

4

INTRODUZIONE AL GDPR | EVOLUZIONE NORMATIVA



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

5

IL REGOLAMENTO UE 2016/679 | GDPR

Regolamento Europeo



Il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea (Serie L 119), è stato pubblicato il **Regolamento Europeo L. 2016/679 GDPR** General Data Protection Regulation



Il Regolamento ha preso applicazione dal **25 maggio 2018**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

6

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

IL REGOLAMENTO UE 2016/679 | GDPR

99
articoli

173
consideranda



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

7

IL REGOLAMENTO UE 2016/679 | GDPR

Cos'è un Regolamento UE?



- È un atto di **portata generale, obbligatorio** in tutti i suoi elementi e **vincolante** (sia per gli Stati che per i singoli)
- Garantisce un **livello di protezione uniforme** in tutta l'Unione Europea
- Garantisce la **certezza del diritto** e la **trasparenza** agli operatori economici
- **«Self-Executing»** = **direttamente applicabile**, ossia NON deve essere recepito → in materia Privacy la Direttiva ha prodotto legislazioni nazionali non sempre armonizzate

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

8

IL REGOLAMENTO UE 2016/679 | GDPR

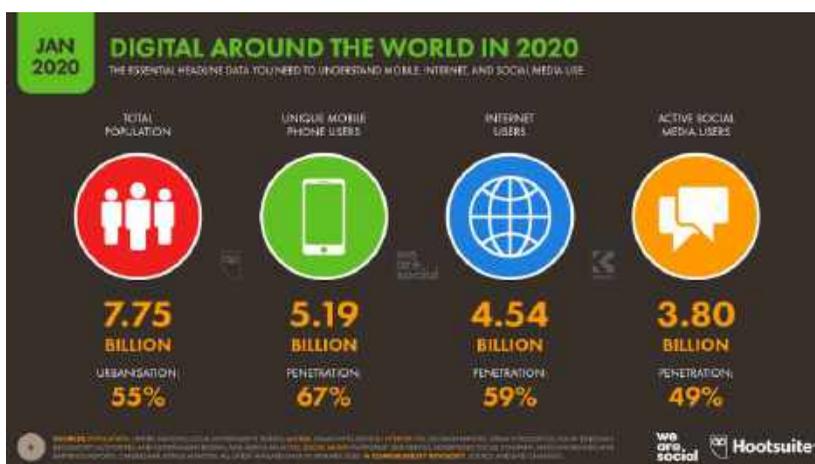
Dalla Direttiva al Regolamento → perché?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

9

REGOLAMENTO UE: PERCHÉ?

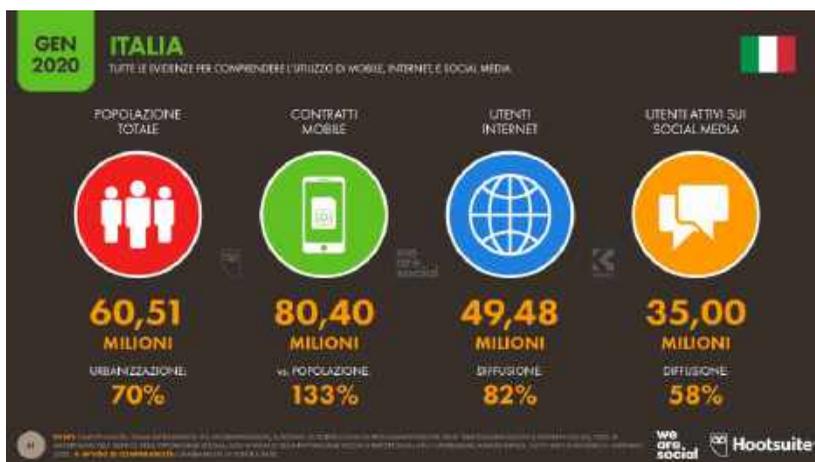


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

10

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

REGOLAMENTO UE: PERCHÉ?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

11

REGOLAMENTO UE: PERCHÉ?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

12

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

RAPPORTO CON LA NORMATIVA NAZIONALE

Considerando 8 stabilisce che ove il GDPR preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri gli stessi possono integrare gli elementi del GDPR nel proprio diritto nazionale:

- nella misura necessaria per la **coerenza**;
- per rendere le **disposizioni nazionali comprensibili** ai soggetti tenuti ad osservarle.

A tal proposito il Parlamento italiano ha delegato il Governo ad intervenire sul **Codice della Privacy** (D.lgs. 196/03) | **Legge 25 Ottobre 2017 n. 163.**



Con il D. Lgs. 101/2018 entrato in vigore il 19 settembre 2018 ha armonizzato la legge nazionale al GDPR | D.Lgs196/03.



13

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

CODICE PRIVACY D.LGS. 196/03 NOVELLATO

→Così come novellato dal **D.Lgs. 101/2018** è destinato a **completare e dare attuazione al Reg. (UE) 2016/679** con l'obiettivo di semplificazione e chiarezza normativa.

Reca **disposizioni per adeguamento nazionale** alle disposizioni del Regolamento.

L'autorità di controllo di cui all'art. 51 GDPR è individuata nel Garante per la protezione dei dati personali «Garante».



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

14

LINEE GUIDA EDPB

Il **Comitato Europeo per la protezione dei dati**, composto dai 27 Garanti UE e dall'EPDS, emette **Linee Guida** su i principali temi legati al GDPR.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

15

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SEDE Piazza Venezia, 11 -
00187 Roma
www.gpdp.it -
www.garanteprivacy.it
E-mail: protocollo@gpdp.it
Fax: (+39) 06.69677.3785
Centralino telefonico:
(+39) 06.69677.1



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

16

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il **Garante per la protezione dei dati personali** è un' **autorità amministrativa indipendente** istituita dalla cosiddetta legge sulla privacy (**legge 31 dicembre 1996, n. 675**) - che ha attuato nell'ordinamento giuridico italiano la **direttiva comunitaria 95/46/CE** - e oggi disciplinata dal Codice in materia di protezione dei dati personali (**d.lg. 30 giugno 2003 n. 196**). Titolo II | rivisto dal D.lgs. 101 | 2018.



È un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile.



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



(da sinistra: Guido Scorza,
Ginevra Cerrina Feroni,
Pasquale Stanzione,
Agostino Ghiglia)

ORGANIGRAMMA GARANTE



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

Pasquale Stanzone,
Presidente
dell'Autorità Garante
dal 29 luglio 2020.
Professore ordinario di
diritto privato.

**Dirigente
Dipartimento Realtà
pubbliche:** Dott.
Francesco Modafferi

LE PRINCIPALI DEFINIZIONI NEL GDPR

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

IL REGOLAMENTO UE 2016/679 | PRINCIPALI DEFINIZIONI

Art. 4 - Definizioni

«**dato personale**» qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»): es. nome, dati di contatto, dati relativi all'ubicazione.

Tipologie di dati personali:

- **Dati personali** c.d. comuni 
- **Categorie particolari di dati personali** (ex dati sensibili)
- **Dati personali relativi a condanne penali e reati**

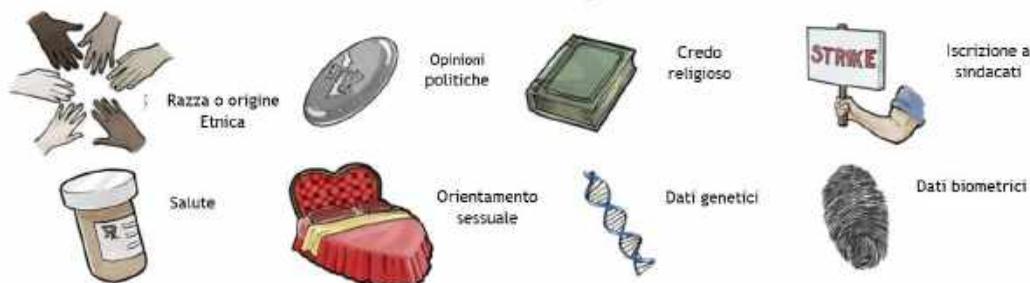


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

21

CATEGORIE PARTICOLARI DI DATI PERSONALI | ART. 9

Treatmento di categorie particolari di dati - Ex dati sensibili



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

22

IL REGOLAMENTO UE 2016/679 | PRINCIPALI DEFINIZIONI

Divieto di trattamento di categorie particolari di dati

Art. 9, par. 1:
DIVIETO trattamento
categorie particolari
di dati personali



Art. 9, par. 2, lett. a)
- j):
DEROGHE a tale
divieto

...il divieto non si applica quando:

g) il trattamento è necessario **per motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri

j) il trattamento è necessario a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica** o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

23

IL REGOLAMENTO UE 2016/679 | PRINCIPALI DEFINIZIONI

Art. 10 – Trattamento dei dati personali relativi a condanne penali e reati



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, **deve avvenire soltanto sotto il controllo dell'autorità pubblica** o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

24

IL REGOLAMENTO UE 2016/679 | PRINCIPALI DEFINIZIONI

Art. 4 - Definizioni

«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



COMUNICAZIONE E DIFFUSIONE | ART. 2 TER D.LGS. 196/03

Attenzione alla differenza tra:

Comunicazione:

Il dare conoscenza dei dati personali a uno o più **soggetti determinati** diversi dall'interessato, dal rappresentante, dal responsabile, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.



Diffusione:

Il dare conoscenza dei dati personali a **soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

COMUNICAZIONE E DIFFUSIONE | ART. 2 TER D.LGS. 196/03

La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi dai particolari o giudiziari, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista da legge o, nei casi previsti dalla legge, da regolamento.

**Se manca la norma
e**

la comunicazione è comunque necessaria

per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali:



- ✓ va fatta comunicazione al Garante che ha 45 gg. per esprimersi
- ✓ se non si esprime entro i 45 gg. la comunicazione può essere iniziata

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

27

TIPOLOGIE DI DATI E DI TRATTAMENTI

Quali dati trattano le Agenzie? Per quali trattamenti?

Dati giudiziari quali casellario giudiziario
per la Gestione delle procedure a evidenza pubblica



Dati relativi lo stato di salute quali disabilità per
la predisposizione di sussidi per lavoratori categoria protetta

Dati personali comuni quali dati di contatto di persone fisiche,
personalità giuridiche e altri ancora, per l'invio di avvisi relativi alle
attività di controllo ufficiali



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

28

TIPOLOGIE DI DATI E DI TRATTAMENTI

Dati idonei a rivelare l'appartenenza sindacale nella gestione del personale in generale



Dati personali comuni quali il livello di istruzione per la ricezione, gestione ed analisi dei curricula



Dati personali comuni quali immagini per la gestione della videosorveglianza



Dati identificativi quali nome e cognome per la gestione delle istanze di accesso civico semplice e generalizzato

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

29

TIPOLOGIE DI DATI E DI TRATTAMENTI

Esempi di trattamenti di dati da parte delle Agenzie

- Gestione del contenzioso Incarichi legali
- Visite ispettive nelle attività produttive per attività istituzionali o su richiesta dell'autorità giudiziaria
- Tenuta e gestione delle caselle di posta elettronica Istituzionale e della casella PEC
- Gestione sezioni Sito Web istituzionale (Albo pretorio, sezione Amministrazione trasparente, pubblicazione bandi e gare, avvisi, delibere e atti)
 - Assunzione a protocollo di tutta la corrispondenza
 - Ricezione dei reclami

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

30

IL REGOLAMENTO UE 2016/679 | PRINCIPALI DEFINIZIONI

Cos'è un Data Breach?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

Art. 4 - Definizioni

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

31

I PRINCIPI FONDAMENTALI PRIVACY

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

32

PRINCIPI APPLICABILI | ART. 5

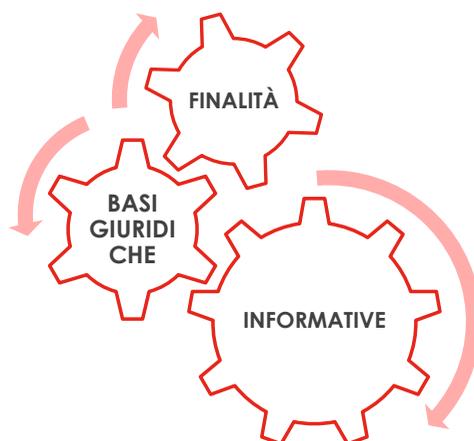


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

33

PRINCIPI APPLICABILI

Liceità, correttezza e trasparenza sono i principi a cui deve ispirarsi ogni operazione di trattamento di dati personali effettuata dal Titolare del trattamento, che è chiamato a rispondere della loro eventuale violazione.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

34

PRINCIPIO DI LICEITÀ

Art. 6 - Principio di Liceità

Il trattamento è **lecito** quando ricorre almeno una delle seguenti **BASI GIURIDICHE** →

A) Consenso dell'interessato

B) Esecuzione di un contratto o misure precontrattuali

C) Adempimento di un obbligo legale

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

35

PRINCIPIO DI LICEITÀ

D) Salvaguardia interessi vitali di un interessato – altra persona fisica

E) **Esecuzione compito di interesse pubblico – esercizio di pubblici poteri**

F) Legittimo interesse del Titolare → a condizione che non prevalgano gli interessi o diritti/libertà fondamentali dell'interessato

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

36

PRINCIPIO DI LICEITÀ

Considerando 47 GDPR

[...] Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, **la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.** [...]



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

37

BASE GIURIDICA P.A.

Art. 2 - ter D.Lgs 196/03 – Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

38

TRATTAMENTO DATI INTERESSE PUBBLICO RILEVANTE

Art. 2 sexies D.Lgs 196/03 - Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante

Il **trattamento di categorie particolari** di dati è **ammesso** –anche in assenza del consenso dell'interessato – purché siano assicurati diritti e libertà fondamentali, **se ciò è reso necessario dall'esistenza di un motivo di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri (Art. 9, par. 2, lett. G) GDPR).

Tali norme devono specificare:

- I tipi di dati che possono essere trattati
 - Le operazioni eseguibili
- Il motivo di interesse pubblico rilevante
- Le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato



TRATTAMENTO DATI INTERESSE PUBBLICO RILEVANTE

L'articolo 2-sexies c. 2 elenca le materie nelle quali l'**INTERESSE PUBBLICO** si considera **RILEVANTE**

Ad esempio:



- Accesso a documenti amministrativi e accesso civico
- Attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano
- Istruzione e formazione in ambito scolastico, professionale, superiore o universitario (ecc.)



PRINCIPIO DI FINALITÀ

Principio della limitazione della finalità → I dati personali raccolti possono essere trattati solo per **finalità determinate, esplicite e legittime**, e non possono essere successivamente trattati per altre finalità incompatibili.

Es. per la selezione dei candidati all'occupazione. 
Es. per la tutela del patrimonio aziendale o l'organizzazione aziendale.

Art. 89 "Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici"

TRASPARENZA E INFORMATIVA

- Articoli di riferimento | **12 - 13 e 14 GDPR**
- **Linea guida su trasparenza**
WP260 REV. 1

Nel GDPR il concetto di trasparenza non è legalistico, ma piuttosto incentrato sull'utente



TRASPARENZA E INFORMATIVA | ART. 12

Cos'è l'informativa privacy? Documento con il quale il Titolare del trattamento informa l'interessato circa le finalità e le modalità del trattamento dei suoi dati personali.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

43

TRASPARENZA E INFORMATIVA | ART. 12

Il titolare del trattamento deve **informare l'interessato** in maniera:

- **concisa**
- **trasparente**
- **intelligibile**
- **facilmente accessibile**
- **linguaggio semplice e chiaro**



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

44

INFORMATIVA PRIVACY | ART. 13 -14 Labor Project® consulenza operativa per l'impresa

Quali informazioni dare?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

45

INFORMATIVA PRIVACY | ART. 13 -14 Labor Project® consulenza operativa per l'impresa



Deve indicare i soggetti

A cui possono essere comunicati i dati personali

Il Garante Privacy nella propria Guida precisa che qualora le **finalità del trattamento dovessero cambiare**, è necessario **informare l'interessato** prima di procedere al trattamento ulteriore

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

46

INFORMATIVA PRIVACY | ART. 13 -14

Ulteriori informazioni

Art. 13

- **Data retention** | periodo di conservazione dei dati;
- **Diritti** esercitabili dall'interessato (es. diritto di accesso etc.).
- Se trattamento si basa sul **consenso** → possibilità di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento fino alla revoca dello consenso;
- **Diritto di reclamo** ad un'autorità di controllo;
- Se la comunicazione di dati è obbligo legale o contrattuale e le possibili conseguenze della mancata comunicazione di tali dati;
- L'esistenza o meno di un **processo decisionale automatizzato** (es. profilazione).

Art. 14

- Stessi diritti informativa ex art. 13 GDPR (da 1. a 6.) +
- **FONTE** da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico
- **Categorie di dati personali** oggetto di trattamento

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

47

CONSERVAZIONE | C.39



I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.

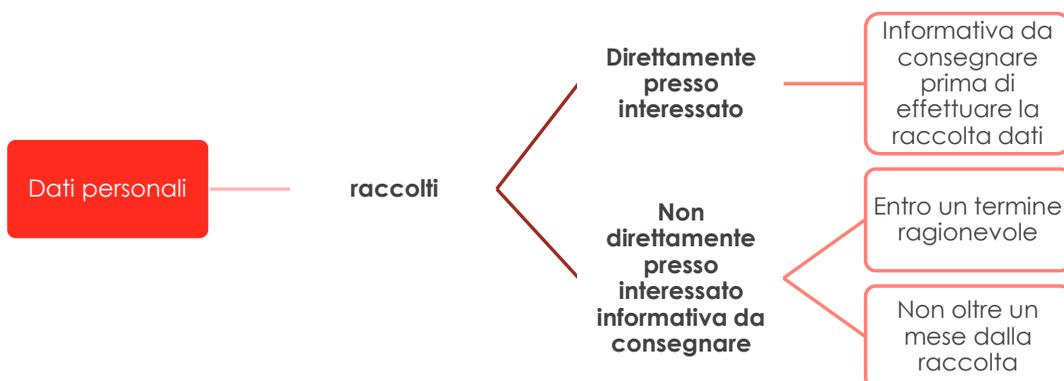
Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il Titolare del trattamento dovrebbe **stabilire un termine per la cancellazione o per la verifica periodica.**

- Fattori: Legge | Linee guida settore.
- Diversi periodi per diverse finalità.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

48

INFORMATIVA PRIVACY | ART. 13 -14



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

49

PRINCIPIO DEL CONSENSO

Art. 7 e C.32,33,42,43 GDPR - Consenso dell'interessato

Il consenso dell'interessato è qualsiasi **manifestazione di volontà:**

- Libera
- Specifica
- Informata
- Inequivocabile
- Esplicita



→ Il consenso dovrebbe coprire tutte le attività di trattamento svolte per lo stesso scopo o finalità.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

50

PRINCIPIO DEL CONSENSO



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

51

PRINCIPIO DEL CONSENSO



Il Titolare del trattamento (Art. 7.1 GDPR), qualora il trattamento sia basato sul consenso, **deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali (onere della prova).**

- Per il Garante Privacy italiano (vedi relazione 2017) l'utilizzo del «**double opt in**» è sicuramente da suggerire come miglior metodo
- All'interno di un **contratto scritto la richiesta di consenso deve essere presentata in modo chiaramente distinguibile e con un linguaggio semplice e chiaro → Facilità di revoca**
- Le azioni positive in chiaro potrebbero includere la selezione con "**flag**" di un'apposita casella (nel caso di un sito Internet) o di una qualsiasi altra dichiarazione o comportamento che indichi chiaramente in questo contesto l'accettazione della persona interessata del trattamento proposto dei suoi dati personali.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

52

PRINCIPIO DEL CONSENSO

Se il **consenso dell'interessato** è prestato nel contesto di una **dichiarazione scritta** la stessa deve:

- Essere redatta in forma comprensibile e accessibile
 - Utilizzare un linguaggio semplice e chiaro
 - Essere priva di clausole abusive
- Portare a conoscenza dell'interessato almeno **identità del Titolare** e la **finalità del trattamento**

Guida del Garante: consenso esplicito per

- Dati particolari (sensibili)
- Scelta automatizzata



INFORMATIVA PRIVACY E CONSENSO

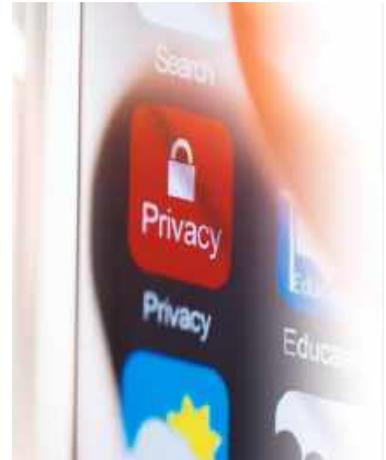
Quando si deve richiedere il consenso?

- Diffusione dell'immagine dell'interessato
- Profilazione
- Marketing diretto
- Cessione del dato a terzi



DIRITTI INTERESSATO | ART. 15 e SS.

-  Diritto di **accesso**
-  Diritto di **rettifica**
-  Diritto alla **cancellazione**
-  Diritto di **limitazione**
-  Diritto di **opposizione**
-  Diritto alla **portabilità**
-  Diritto di **proporre reclamo** a un'autorità di controllo



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

55

DIRITTO DI ACCESSO | ART. 15

Diritto di avere **conferma** che sia o meno in corso un trattamento di dati personali e di aver conoscenza ad esempio di:

-  **finalità** del trattamento
-  le **categorie di dati** personali in questione
-  periodo di **conservazione** dei dati
-  chiedere la **rettifica o la cancellazione** dei dati personali o la **limitazione** del trattamento o opporsi
-  conoscere l'esistenza processo decisionale automatizzato, compresa la **profilazione**
-  **ambito di comunicazione** (paesi terzi o organizzazioni internazionali)

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

56

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

ACCESSO A DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO



Il nuovo **art. 59** Codice Privacy prevede il “raccordo” delle normative *in materia di accesso a documenti amministrativi* contenuta nella legge n. 241 | 90 e *accesso civico (semplice o generalizzato)* di cui al decreto legislativo 33 | 2013, con le regole e i principi in materia di protezione dei dati personali.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

57

ACCESSO A DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

58

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

ACCESSO A DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e **va contemperato con altri diritti fondamentali**, in ossequio al **principio di proporzionalità**.

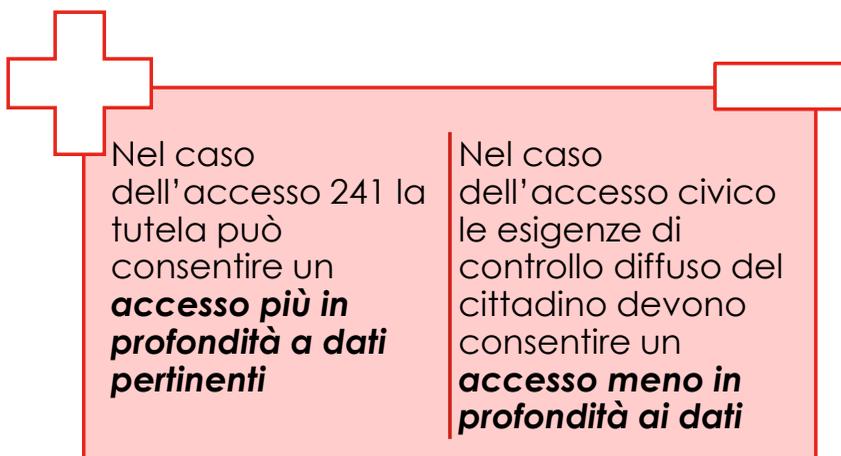
Realizzare un **equo bilanciamento fra i diritti dell'istante e la tutela della riservatezza del terzo** i cui dati compaiono nella documentazione cui si chiede di accedere.

Il Codice Privacy ha privilegiato la tutela alla trasparenza rispetto alla tutela alla privacy (art. 59 che rimanda alle normative in materia di trasparenza).
Eccezione: diritti alla salute, alla vita sessuale, all'orientamento sessuale

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

59

ACCESSO A DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO



Nel caso dell'accesso 241 la tutela può consentire un **accesso più in profondità a dati pertinenti**

Nel caso dell'accesso civico le esigenze di controllo diffuso del cittadino devono consentire un **accesso meno in profondità ai dati**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

60

ACCESSO A DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

Salute

Vita sessuale

Orientamento sessuale

Il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di **rango almeno pari ai diritti dell'interessato**, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Presuppone una **valutazione in concreto**, in modo da evitare per le amministrazioni, gli altri destinatari delle richieste e per il giudice stesso in caso di impugnazione, *«il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in contesa»*, che tenga conto anche dei **principi di necessità e pertinenza e non eccedenza dei dati**.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

61

INTERESSATO E PROCESSO DECISIONALE AUTOMATIZZATO

Processo decisionale automatizzato relativo alle persone fisiche, **compresa la profilazione – Art. 22**



L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

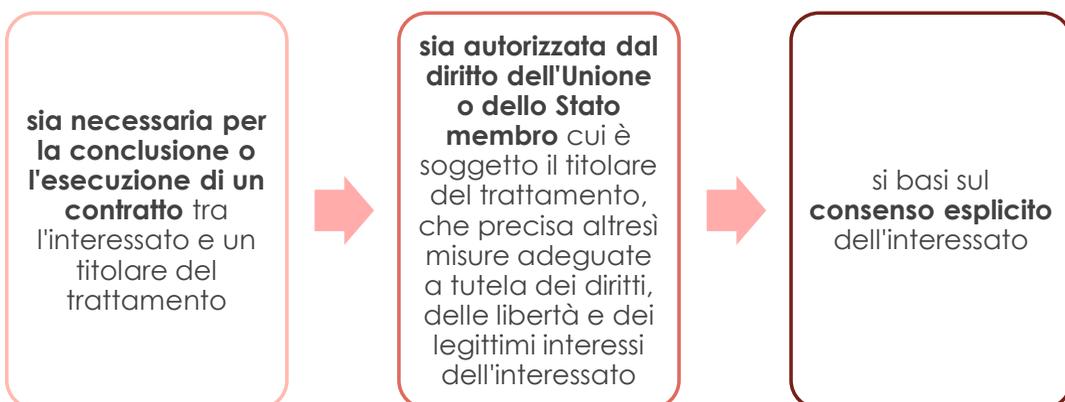


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

62

INTERESSATO E PROCESSO DECISIONALE AUTOMATIZZATO

→ A meno che:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

63

INTERESSATO E PROFILAZIONE

Art. 21

l'interessato deve essere **informato** in merito al **diritto di opporsi alla profilazione** in modo chiaro ed evidente

→ **chiunque ha il diritto di opporsi alla profilazione**



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

64

RISPOSTA ALL'INTERESSATO | DIRITTI

L'interessato ha diritto ad una risposta dal Titolare del trattamento riguardo l'esercizio dei loro diritti (artt. 15-22 GDPR e comunicazione data breach (art. 34 GDPR):



Senza ingiustificato ritardo e, comunque, **al più tardi entro un mese dal ricevimento della richiesta** da parte dell'interessato.

Nota bene: tale termine può essere prorogato di due mesi, se necessario, tenuto conto della **complessità e del numero delle richieste e informando l'interessato dei motivi del ritardo.**

Se la richiesta avviene con mezzi elettronici ove possibile le risposte sono fornite nella medesima modalità

RISPOSTA ALL'INTERESSATO | DIRITTI

Qualora il Titolare del trattamento **nutra ragionevoli dubbi** circa l'identità della persona fisica che presenta la richiesta **può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.**



Le richieste dell'interessato sono gratuite (art. 12.5 GDPR)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

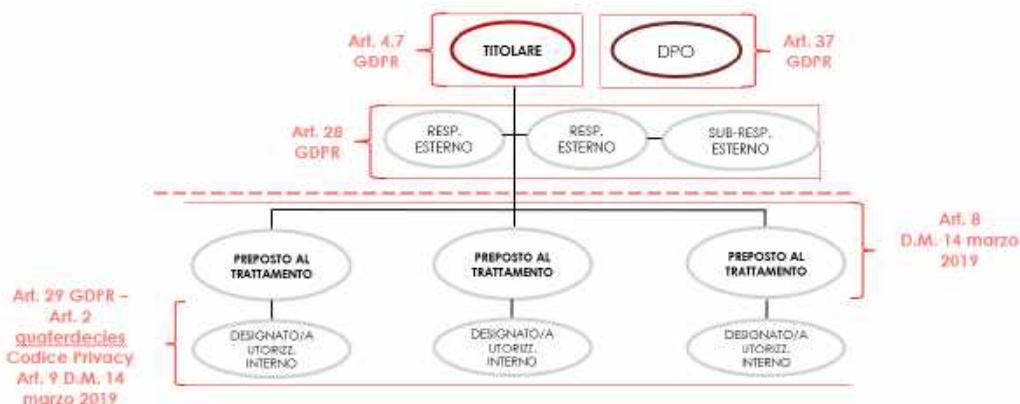
67

IL SISTEMA ORGANIZZATIVO PRIVACY

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

68

IL SISTEMA ORGANIZZATIVO PRIVACY



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

69

IL SISTEMA ORGANIZZATIVO PRIVACY

Regolamento Europeo (EN)	Regolamento Europeo (IT)	T.U. Privacy Italiano D.Lgs. 196/03
Data Controller	Titolare del Trattamento	Titolare del Trattamento da GDPR
Data Processor	Responsabile del Trattamento	Responsabile del Trattamento da GDPR
Persons Authorised to Process (non definito)	Incaricato del Trattamento/ Persona autorizzata al trattamento	Persone fisiche designate art. 2 quaterdecies
Data Protection Officer	Responsabile della Protezione dei Dati	Responsabile della Protezione dei Dati Autorità Giudiziaria Art. 2 sexiesdecies

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

70

TITOLARE DEL TRATTAMENTO | GDPR

Art. 24 - Responsabilità del titolare del trattamento

Il titolare deve mettere in atto **misure tecniche e organizzative adeguate** in conformità al regolamento sulla base di:



- **Natura**
- **Ambito di applicazione**
- **Contesto**
- **Finalità** del trattamento
- **Rischi** probabili



garantiscono che il trattamento sia conforme al regolamento
e
devono essere riesaminate e aggiornate quando necessario

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

71

TITOLARE DEL TRATTAMENTO | GDPR

Il Titolare del trattamento è l'Agenzia Regionale per la Protezione dell'Ambiente, *nella persona del/della Direttore/Direttrice generale, suo/sua rappresentante legale pro tempore.*

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

72

PRINCIPIO DI ACCOUNTABILITY

Principio di accountability → Responsabilizzazione del Titolare del trattamento, il quale deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, *indicando obbligatoriamente – per ognuno di essi – una serie “nutrita” di informazioni, tali da assicurare e comprovare – per ciascuna operazione – la conformità alle disposizioni del Regolamento.*



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

73

MISURE DI SICUREZZA

Art. 32 GDPR

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



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

74

RESPONSABILE DEL TRATTAMENTO | GDPR

Art- 28 - Il Titolare del trattamento **può designare uno o più**



Responsabili del trattamento

- **che collaborano con il Titolare per assicurare:**
 - misure tecniche e organizzative adeguate
- trattamento conforme al Regolamento
 - tutela dei diritti dell'interessato



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

75

RESPONSABILE DEL TRATTAMENTO | GDPR

EDPB - Linee-guida 07/2020 su titolare e responsabile del trattamento

Quali elementi sono da prendere in considerazione nella scelta?

- le conoscenze specialistiche (*ad esempio, la competenza tecnica in materia di misure di sicurezza e di violazione dei dati – data breach*);
- l'affidabilità;
- le risorse;
- l'eventuale adesione a un codice di condotta o a un meccanismo di certificazione approvato.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

76

RESPONSABILE DEL TRATTAMENTO | GDPR

Titolare

contratto o da altro atto giuridico

Responsabile

Vincola il Responsabile al Titolare del trattamento e stipula:

- la materia disciplinata
- la durata del trattamento
- la finalità del trattamento
- il tipo di dati personali trattati
- le categorie di interessati
- gli obblighi del titolare
- i diritti dell'interessato



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

77

RESPONSABILE DEL TRATTAMENTO | GDPR

Il **contratto** che regola il trattamento dati da parte del **Responsabile** garantisce che questi:

tratti i dati personali soltanto su **istruzione documentata del titolare** del trattamento



garantisca la **riservatezza** anche da parte degli autorizzati



adotti tutte le **misure di sicurezza adeguate** | ART. 32



assista il Titolare nel **rispetto degli obblighi** previsti dal Regolamento



cancelli tutti i dati personali dopo il trattamento o li **restituisca** al titolare



metta **a disposizione** del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

78

RESPONSABILE DEL TRATTAMENTO | GDPR

E in caso di violazione dei dati personali?

- ✓ Il responsabile deve **informare** il titolare ogni volta che scopre una violazione dei dati personali;
- ✓ Deve **aiutare** il titolare nella segnalazione all'autorità di controllo e nella comunicazione agli interessati.



La notifica del responsabile del trattamento al titolare del trattamento dovrebbe avvenire **senza indebito ritardo**



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

79

RESPONSABILE DEL TRATTAMENTO | GDPR

... a tal fine l'EDPB raccomanda che il contratto indichi:

1. Il periodo di **tempo** specifico per la notifica (ad esempio in numero di ore)
2. il punto di **contatto** per tali notifiche
3. con che **modalità** il responsabile del trattamento deve effettuare la comunicazione al titolare (es. allegando modello)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

80

RESPONSABILE DEL TRATTAMENTO | GDPR

DPO SÌ O NO?



Qualora un'autorità pubblica debba subappaltare attività di trattamento ad organismi privati (es. attività contabili) **sarebbe quantomeno opportuno** scegliere un responsabile che ha designato un RPD | DPO, o obbligarne uno, che ancora manca di questa figura, a designarla.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

81

SUB- RESPONSABILE DEL TRATTAMENTO | GDPR



Il Responsabile del trattamento nominato non può ricorrere ad un altro Responsabile senza previa **autorizzazione scritta, specifica o generale**, del Titolare del trattamento.

NB:
Il Titolare può sempre opporsi

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

82

SUB- RESPONSABILE DEL TRATTAMENTO | GDPR

Chi risponde?



Quando un Responsabile del trattamento **ricorre a un altro Responsabile**, il primo Responsabile risponde nei confronti del Titolare.

Qualora l'**altro responsabile** del trattamento **ometta di adempiere ai propri obblighi** in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

83

POLITICA DI SICUREZZA | SUBAPPALTO

Se il trattamento viene demandato ad un «secondo» Responsabile deve essere adottata una **POLITICA DI SICUREZZA** che garantisca:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

84

POLITICA DI SICUREZZA

Al fine di garantire la sicurezza rivestono un ruolo fondamentale gli **AUDIT | CHECKLIST | VERIFICHE** a cadenza periodica. *Esempio:*



Domande

Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti mediante lettera di incarico (art 29 GDPR)?

Tutte le persone autorizzate al trattamento partecipano, su base annuale, a corsi di formazione incentrati sugli obblighi previsti dalle normative vigenti in tema di Protezione dei Dati?

Avete adottato un registro delle attività di Trattamento (art 30 GDPR) in qualità di Responsabile? Se così fosse, questo registro è sempre aggiornato?

È stato nominato il Data Protection Officer?

Avete adottato misure organizzative interne volte a prevenire / gestire eventuali violazioni in merito al trattamento di dati personali da parte degli autorizzati al trattamento dei dati personali (procedura di data breach ai sensi degli artt. 33 e 34 GDPR)?

AUTORIZZATI AL TRATTAMENTO | GDPR e D.LGS. 196/03

Art. 29 GDPR e Art. 2 quaterdecies D.Lgs. 196/03 armonizzato



disciplinano la figura
dell'autorizzato/designato al trattamento

Il titolare o il responsabile del trattamento individuano le **modalità più opportune** per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta → lettere autorizzati



RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

**Artt. 37 – 39
GDPR**



Chi è?

Il DPO (Data Protection Officer) è una figura introdotta con il GDPR, e rappresenta un professionista (interno o esterno) con competenze normative, informatiche, gestionali, di risk management e di analisi dei processi, etc. il cui compito principale è di **vigilare sulla corretta ed effettiva osservanza delle norme in materia di privacy.**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

87

REGISTRO DEI TRATTAMENTI

Art. 30 - Ogni **Titolare del trattamento** e, ove applicabile, il rappresentante designato deve tenere un **Registro delle attività di trattamento** svolte sotto la propria responsabilità.

- Ogni **Responsabile del trattamento** designato deve tenere un **Registro delle attività di trattamento** svolte sotto la propria responsabilità.

Finalità C82:

Documentare dinanzi
all'Autorità
di controllo la conformità
dell'organizzazione alle norme
del Regolamento Privacy UE



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

88

REGISTRO DEI TRATTAMENTI



Il Registro deve contenere, **in forma scritta (anche elettronica)** una serie di informazioni e deve essere tenuto a disposizione dell'Autorità Garante che ne faccia richiesta.

Registro del Titolare → elementi obbligatori ex art. 30 GDPR

REGISTRO DEI TRATTAMENTI

Il registro del Responsabile deve invece contenere le seguenti informazioni:



REGISTRO DEI TRATTAMENTI ART. 30

Divisione
Ufficio personale

Azienda
Posta elettronica X Archivio cartaceo X
Software (o) fornito dal CDL X

Finalità
Comparto X Adempimento obblighi di legge X

Contributo del trattamento
Non presente

Categorie di soggetti interessati
Dipendenti X

Categorie di dati trattati
Dati Anagrafici X Dati identificativi, economici e fiscali X
Dati sensibili - Dati idonei a rivelare caratteristiche o abitudini psico-fisiche X
Dati sensibili - Dati idonei a rivelare lo stato di disabilità X
Altre informazioni strettamente connesse allo svolgimento dell'attività lavorativa (quali la tipologia del contratto, la mansione, le ferie o i permessi individuali, l'attribuzione dei premi, etc.) X

Responsabili
Consulente del Lavoro L.J. X

Categorie di destinatari
Soggetti per attività di consulenza amministrativo-contabile, contrattuali, precontrattuali e fiscali X
Soggetti dedicati ad attività di assistenza informatica X
Studio di elaborazione delle buste paga X
Autorizzati art. 29 X

Nazioni extra-UE
Laziosi extra UE

Organizzazioni internazionali

Caratteristiche
Caratteristiche adeguate

Misure di sicurezza tecniche e organizzative
Backup X
Lattine agli automezzi art. 29 rinnovate periodicamente X
Formazione periodica del personale X
Password cambiate almeno ogni 3 mesi X

Esempio...

**Finalità:
GESTIONE DEL
PERSONALE**

Tempo di conservazione dei dati

non Anagrafici
30 anni dalla cessazione del rapporto di lavoro salvo diverso d... X

non Anagrafici, economici e fiscali
30 anni dalla cessazione del rapporto di lavoro salvo diverso d... X

Altre informazioni strettamente connesse allo svolgimento dell'attività lavorativa (quali la tipologia del contratto, la mansione, le ferie o i permessi individuali, l'attribuzione dei premi, etc.)
30 anni dalla cessazione del rapporto di lavoro salvo diverso d... X

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

91

TRASFERIMENTO DATI ESTERO



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

92

TRASFERIMENTI VERSO PAESI TERZI (NON SEE)

Il trasferimento di dati personali verso
un paese terzo o un'organizzazione
internazionale



è lecito



se il Titolare e il Responsabile del
trattamento possono far valere
specifiche garanzie → **Artt. da 45 a 49
del GDPR**



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

93

TRASFERIMENTI VERSO PAESI TERZI (NON SEE)

Trasferimenti extra UE

Decisione di adeguatezza – **Art. 45
GDPR**

Garanzie adeguate – **Art. 46 GDPR**

Norme vincolanti d'impresa – **Art.
47 GDPR**

Deroghe – **Art. 49 GDPR**

Condizioni per il
**trasferimenti verso
un paese terzo o
un'organizzazione
internazionale:**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

94

TRASFERIMENTI DATI EXTRA UE

Art. 45 - Trasferimento sulla base di una decisione di adeguatezza



Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale **è ammesso** se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione **garantiscono un livello di protezione adeguato (es. Svizzera).**

In tal caso il trasferimento non necessita di autorizzazioni specifiche.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

95

DECISIONE DI ADEGUATEZZA | ART. 45 GDPR

Paesi terzi ad oggi riconosciuti «safe» dalla Commissione Europea ed autorizzati dal Garante

- Andorra
- Argentina
- Australia PNR
- Canada
- Isole Faer Oer
- Giappone (23/02/2019)
- Bailato di Guernsey
 - Isole di Man
- Bailato di Israele
 - Jersey
- Nuova Zelanda
- Svizzera
- Repubblica Orientale dell'Uruguay
 - USA Privacy Shield*
 - USA PNR



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

96

TRASFERIMENTI DATI EXTRA UE

GARANZIE ADEGUATE, l'art. 46 GDPR **prevede diversi meccanismi**, tra loro alternativi, atti a garantire la liceità dei trasferimenti:

- A. uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici
- B. le norme vincolanti d'impresa | BCR | in conformità dell'articolo 47
- C. le clausole tipo di protezione dei dati adottate dalla Commissione
- D. le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione
- E. un codice di condotta (...) o
- F. un meccanismo di certificazione (...)

DEROGHE IN SPECIFICHE SITUAZIONI | ART. 49 GDPR



In assenza di una **decisione di adeguatezza** o di **garanzie adeguate** il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale può essere comunque ammesso se sussistono le **condizioni previste dall'art. 49** GDPR.

DEROGHE IN SPECIFICHE SITUAZIONI | LINEE GUIDA 2/2018

TEST DI NECESSITÀ



L'utilizzo delle eccezioni previste dall'art. 49 GDPR richiede che sia valutata la **necessità** di tale trasferimento per una determinata finalità. Il **test di necessità** deve essere applicato per verificare la possibilità di utilizzo delle deroghe ex Art. 49, par. 1, lett. b), c), d), e) ed f)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

99

DEROGHE IN SPECIFICHE SITUAZIONI | ART. 49 GDPR

Quali sono le specifiche situazioni?

A) l'**interessato ha esplicitamente acconsentito al trasferimento**, dopo essere stato informato dei possibili rischi del trasferimento per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate

B) il trasferimento è **necessario all'esecuzione di un contratto concluso tra l'interessato e il Titolare del trattamento**, ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

C) il trasferimento è **necessario per la conclusione o l'esecuzione di un contratto** stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

100

DEROGHE IN SPECIFICHE SITUAZIONI | ART. 49 GDPR

D) il trasferimento è **necessario per importanti motivi di interesse pubblico**, riconosciuti dal diritto dell'Unione Europea o di uno Stato membro

E) il trasferimento è **necessario per accertare, esercitare o difendere un diritto in sede giudiziaria**

F) il trasferimento sia **necessario per tutelare gli interessi vitali dell'interessato o di altre persone**, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso

G) il **trasferimento sia effettuato a partire da un registro** che mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, a condizione che sussistano i requisiti per la consultazione

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

101

DEROGHE IN SPECIFICHE SITUAZIONI | ART. 49 GDPR

Le condizioni indicate in precedenza nei punti a), b) e c), **non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.**

In mancanza di una decisione di adeguatezza, il diritto dell'UE o dello Stato membro può fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un Paese terzo o un'organizzazione internazionale **per importanti motivi di interesse pubblico**, con obbligo di notifica delle disposizioni agli Stati membri.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

102

TRASFERIMENTO DATI | U.S.A.

Cronistoria normativa

12 Luglio 2016

La Commissione Europea adotta una decisione in merito al c.d. «**Privacy Shield**» operativo dal 1 agosto 2016 che dispone le **regole** da osservare per il **trasferimento dei dati verso gli U.S.A.** e che impone alle imprese americane obblighi più stringenti di tutela dei dati personali di persone fisiche europee



Il Privacy Shield segue alla sentenza della Corte di Giustizia dell'Unione Europea del 6 ottobre 2015, che ha dichiarato invalida la precedente decisione della Commissione Europea del 2000 sullo scambio di dati fra UE e USA, il cd. «Safe Harbour».

TRASFERIMENTO DATI | U.S.A.

• La sentenza SCHREMS II - causa C-311/18



Il 16/07/2020 la CGUE si è pronunciata in merito al regime di trasferimento dei dati tra UE e USA, dichiarando **invalida la decisione 2016/1250** della Commissione **sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy.**

La sentenza ha anche creato incertezza rispetto all'applicazione delle clausole contrattuali standard (CSS) e alle Binding Corporate Rules (BCR), rendendo **critico il trasferimento dei dati extra SEE.**

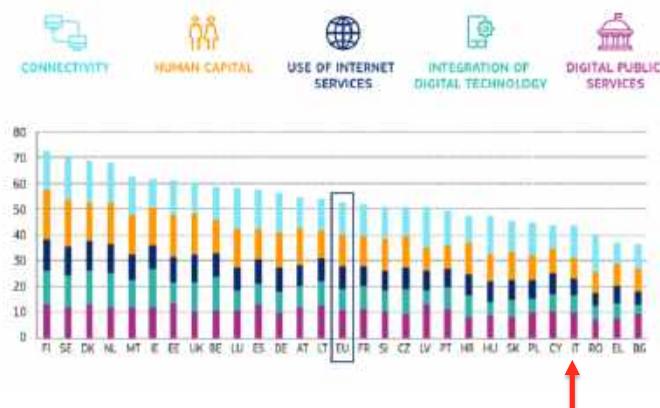
TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE, CRITICITÀ E SOLUZIONI

105

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

The Digital Economy and Society Index (DESI) è un indice composto che riassume gli indicatori pertinenti sulla performance digitale dell'Europa e segue l'evoluzione degli Stati membri dell'UE in materia di competitività digitale.

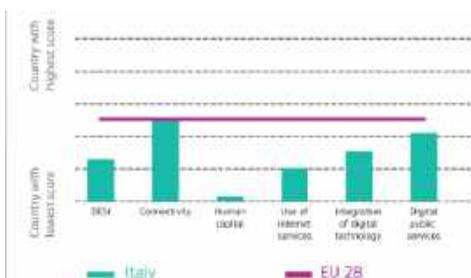


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

106

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY



La pubblica amministrazione italiana tenta da oltre venti anni di stare al passo della rivoluzione digitale che ormai si è impadronita della società, ma i dati sono sempre impietosi. Siamo a ridosso degli ultimi – ce lo ricorda anche il Desi 2020 – i quali tra l'altro crescono velocemente e si avvicinano con il sempre più pressante rischio di superamento.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

107

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Art. 2, c. 1 del Codice dell'Amministrazione Digitale (CAD)

«Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in **modalità digitale** e si organizzano ed agiscono a tale fine utilizzando le modalità più appropriate, e nel modo più adeguato al soddisfacimento degli interessi degli utenti, le tecnologie dell'informazione e della comunicazione»

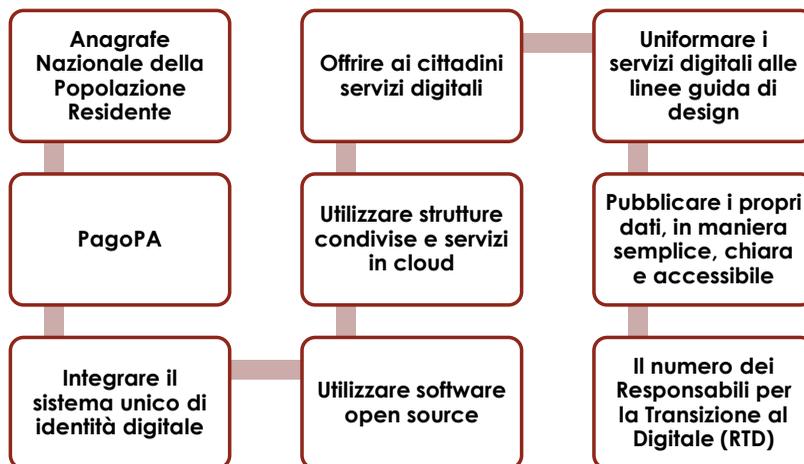


Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

108



TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

109



TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Utilizzare software open source



Questo è un obbligo stabilito nel CAD. Sul cruciale tema del **risparmio** questo è tema è basilare. In ogni evenienza è indispensabile fare una valutazione comparativa per verificare che non sia già disponibile un prodotto sia rilasciato da altre PA ovvero reperibile con licenza *open source*.

MA ATTENZIONE ALLA SICUREZZA

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

110

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Utilizzare strutture condivise e servizi in cloud



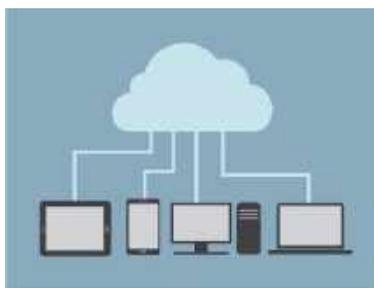
Le PA non dovrebbero investire più su servizi in locale **abbandonando progressivamente la gestione diretta di CED**. Il *cloud* in questi scenari garantisce forti economie di scala, ma va gestita opportunamente la protezione dei dati personali in conformità al GDPR.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

111

PRINCIPIO DEL CLOUD FIRST

Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2020 - 2022



Dal 1
aprile
2020

Nella fase di definizione di un **nuovo** progetto e/o sviluppo di servizi, le PP.AA sono tenute ad adottare il paradigma **Cloud First**.

Le PA sono obbligate ad acquisire **solo servizi cloud qualificati**, rinvenibili nel Cloud Marketplace gestito da AgID.

AgID ha individuato i **requisiti per la qualificazione** di soluzioni SaaS, suddividendoli in tre classi: requisiti preliminari, organizzativi e specifici.

Tale procedura consente alle Amministrazioni di utilizzare, nell'ambito del Cloud della PA, soluzioni SaaS in possesso di **un set minimo di requisiti comuni**.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

112

PRINCIPIO DEL CLOUD FIRST

I **requisiti specifici** per la qualificazione sono a loro volta suddivisi in:

requisiti di sicurezza, privacy e protezione dati
(RS)

requisiti di performance e scalabilità (RPS)

requisiti di interoperabilità e portabilità (RIP)

requisiti di conformità legislativa (RCL)

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Offrire ai cittadini servizi digitali



L'integrazione di SPID, pagoPA e ANPR affiancata alla semplificazione dei procedimenti amministrativi mettono in condizione la PA di **riprogettare i propri servizi e di proporli direttamente online**. Questo è il punto più dolente della trasformazione digitale. **I servizi sono progettati digitalizzando procedimenti analogici con i problemi che ne derivano.**

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Uniformare i servizi digitali alle linee guida di design

I servizi digitali ai quali i cittadini sono ormai abituati sono rispondenti ai bisogni reali, semplici, rapidi e intuitivi. Devono essere applicati nella PA sia per reperire informazioni sulla pagina *web* dell'amministrazione, sia per servizi più complessi di tipo interattivo.

Linee guida di design per i servizi digitali della PA

*La trasparenza sui siti web della PA -
Linee guida del Garante*

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

115

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

Pubblicare i propri dati, in maniera semplice, chiara e accessibile

Questo principio è **la base della trasparenza** che è un dovere per tutta la PA. Stiamo parlando in particolare dei dati aperti o *open data*, tramite i quali il cittadino può far valere il diritto di avere accesso alle informazioni, agli atti e ai documenti pubblici in genere.



Non sempre l'amministrazione è interattiva e spesso si oppone il diritto alla protezione dei dati personali.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

116

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

117

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

La **diffusione di dati personali da parte dei soggetti pubblici** è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento.



Pertanto, in relazione all'operazione di diffusione, occorre che le pubbliche amministrazioni, prima di mettere a disposizione sui propri siti web istituzionali informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, **verifichino che la normativa in materia di trasparenza preveda tale obbligo.**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

118

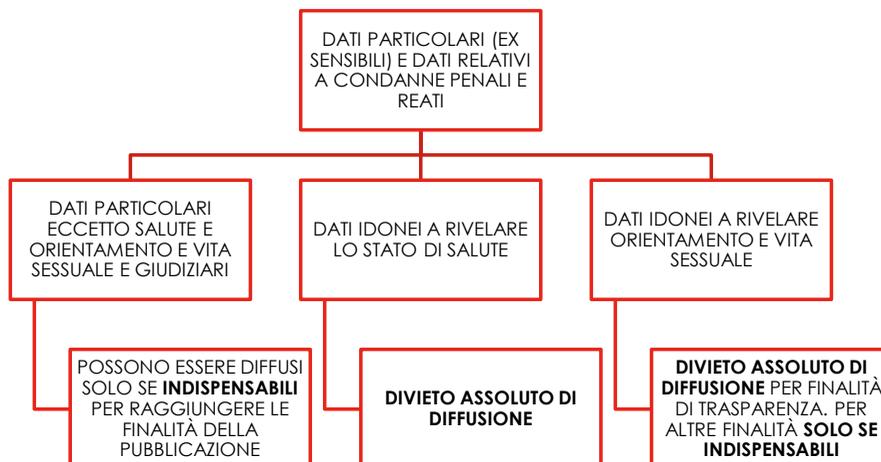
TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

119

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

120

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

TRASFORMAZIONE DIGITALE DELLA PA E PRIVACY

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo **procedendo all'anonimizzazione** dei dati personali eventualmente presenti.

**SOSTITUIRE IL NOME E
COGNOME
DELL'INTERESSATO CON LE
SOLE INIZIALI È DI PER SÉ
INSUFFICIENTE**



OSCURAMENTO

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

121

DOMANDE



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

122

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

IL DOCENTE

AVV. ELISA MARINI



Avvocato. Formatrice, esperta nella consulenza in materia di Privacy e contrattualistica. Ha conseguito la certificazione UNI 11697 come Data Protection Officer ed è Valutatore Interno ISO 27001 qualificato da Bureau Veritas Italia SpA.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

123



GRAZIE PER L'ATTENZIONE

www.laborproject.it

124

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE



IL GDPR NELLA PUBBLICA AMMINISTRAZIONE, CRITICITÀ E SOLUZIONI

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

INDICE ARGOMENTI

- 1. Inquadramento Normativo**
- 2. Le principali definizioni nel GDPR**
- 3. I Principi fondamentali Privacy**
- 4. Il Sistema Organizzativo Privacy**
- 5. Trasformazione digitale della PA e privacy**
- 6. La sicurezza dei dati nella PA**
- 7. Il DPO – RPD nella pubblica amministrazione**
- 8. Il sistema sanzionatorio**
- 9. Provvedimenti privacy (cenni): Videosorveglianza e Biometria**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

126

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

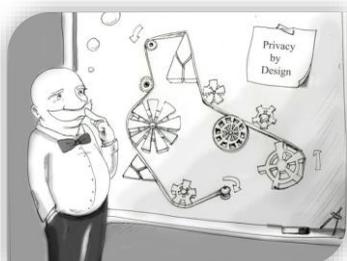
LA SICUREZZA DEI DATI NELLA PA

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

127

PRIVACY BY DESIGN & DEFAULT | ART. 25

Art. 25 - Privacy by design



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

In che cosa consiste?

Nell'obbligo in capo al Titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate alla protezione dei dati personali

Quando deve avvenire?

Sin dall'origine, prima di procedere al trattamento dei dati, sia nel corso di tutto il trattamento stesso

Come scegliere tali misure? Tenendo conto:

- dello stato dell'arte e dei costi di attuazione
- della natura, dell'ambito di applicazione, del contesto e finalità
- dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

128

PRIVACY BY DESIGN & DEFAULT | ART. 25

Art. 25 - Privacy by default



In che cosa consiste?

Nella necessità di adottare, per impostazione predefinita, meccanismi tali da garantire che siano trattati **solo i dati necessari** per ogni specifica finalità di trattamento.

Il principio si estende alla quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Qual è lo scopo?

In particolare dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

129

PRINCIPI APPLICABILI

Principi

Principio della minimizzazione dei dati / di necessità / di pertinenza e non eccedenza → Devono essere raccolti unicamente i dati personali necessari per raggiungere la finalità prestabilita. I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

Principio di esattezza / di proporzionalità → I dati personali devono essere esatti e, se necessario, aggiornati.

Principio dell'integrità e della riservatezza → I dati personali devono essere trattati così da garantire un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate. Es: i dati personali possono essere protetti rendendoli non identificabili con cifratura o pseudonimizzazione

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

130

PRIVACY BY DESIGN & DEFAULT | ART. 25

Viene richiesto al Titolare di configurare il trattamento **prevedendo fin dall'inizio le garanzie indispensabili** «al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati».

Tutto questo **deve avvenire dall'origine**, prima di procedere al trattamento dei dati vero e proprio **e richiede, quindi, un'analisi preventiva** e un impegno applicativo da parte dei Titolari che devono sostanziarsi in una serie di attività specifiche dimostrabili.



PRIVACY BY DESIGN & DEFAULT | ART. 25

- Il 20/10/2020, conclusa la fase di consultazione pubblica, l'EDPB ha adottato le **linee guida in materia di data protection by design e by default**.

Titolari ed interessati trarranno maggiori vantaggi dalla protezione dei dati di default se la protezione dei dati in fase di progettazione viene attuata contemporaneamente - e viceversa.



I concetti sono complementari fra loro

LINEE GUIDA EDPB - PRIVACY BY DESIGN

Il Titolare adotta **misure tecniche e organizzative adeguate**, volte ad attuare i principi di protezione dei dati e ad integrare le **necessarie garanzie** nel trattamento, al fine di soddisfare i requisiti e tutelare i diritti e le libertà delle persone interessate.

Sia le misure adeguate che le garanzie necessarie sono destinate a servire lo stesso scopo di:

- *tutelare i diritti degli interessati e*
- *assicurare che la protezione dei loro dati sia integrata nel trattamento.*

LINEE GUIDA EDPB - PRIVACY BY DESIGN

Le misure e le garanzie necessarie devono essere idonee a raggiungere lo scopo previsto, vale a dire **devono attuare efficacemente i principi di protezione dei dati**. Il requisito dell'adeguatezza è quindi strettamente legato al **requisito dell'efficacia**.

“Effectiveness is at the heart of the concept of data protection by design”

LINEE GUIDA EDPB - PRIVACY BY DESIGN

Come verificare e dimostrare l'efficacia delle misure adottate?

key
performance
indicators



Dimostrazione
logica delle
scelte

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

135

LINEE GUIDA EDPB - PRIVACY BY DESIGN

✓ Il controllore può scegliere degli «indicatori chiave» o «**key performance indicators (KPI)**» per dimostrare l'efficacia.

I KPI possono essere:

- **Quantitativi** es. la riduzione dei reclami ricevuti, o la riduzione dei tempi di risposta agli interessati
- **Qualitativi** es. la valutazione delle prestazioni da parte di esperti, l'uso di scale di classificazione

✓ In alternativa ai KPI, i titolari possono dimostrare l'effettiva attuazione dei principi **fornendo la logica** che sta alla base la loro valutazione dell'efficacia delle misure e delle salvaguardie scelte.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

136

LINEE GUIDA EDPB - PRIVACY BY DESIGN

L'EDPB fornisce indicazioni sui criteri da utilizzare per implementare le misure, dallo stato dell'arte ai costi di attuazione.

Per quanto riguarda il profilo di attuazione temporale, prendere in considerazione **quanto prima** il principio di privacy by design è fondamentale per garantire l'efficacia delle misure e l'effettiva tutela degli interessati. Così come è fondamentale mantenere ed aggiornare le misure nel corso del trattamento.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

137

LINEE GUIDA EDPB - PRIVACY BY DEFAULT

Con «BY DEFAULT» si fa generalmente riferimento ad una condizione pre-esistente, un «preset» o «factory preset» in informatica.

Anche nell'ambito privacy il concetto si riferisce ad una configurazione di valori o di opzioni del trattamento che sono già impostate e che **influiscono, fin dal principio**, sulla quantità di informazioni raccolte, sulla durata del trattamento, sulla conservazione dei dati nel tempo, sulla loro accessibilità.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

138

LINEE GUIDA EDPB - PRIVACY BY DEFAULT

Es.

Se il titolare utilizza un software di terze parti, dovrebbe dapprima svolgere un risk assessment sul prodotto ed assicurarsi che eventuali funzioni aggiuntive, non necessarie in relazione alle finalità perseguite, vengano disattivate.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

139

MISURE DI SICUREZZA TECNICHE

Misure di sicurezza tecniche 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.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

140

MISURE DI SICUREZZA TECNICHE

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo **dei rischi presentati dal trattamento** che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso**, in modo accidentale o illegale, **a dati personali trasmessi, conservati o comunque trattati.**



MISURE DI SICUREZZA | P.A. - AgID



Le **pubbliche amministrazioni** sono tenute al rispetto delle misure minime di sicurezza ICT emanate dall'**AgID** – Agenzia per l'Italia digitale nel 2017



valutare e migliorare il livello di sicurezza informatica delle amministrazioni, con l'obiettivo di contrastare le minacce informatiche.

MISURE DI SICUREZZA | P.A. - AgID

In base alla complessità del sistema informatico ed alla realtà organizzativa dell'Amministrazione pubblica, le «**Misure minime di sicurezza informativa per la P.A.**» prevedono i seguenti livelli di attuazione:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

143

MISURE DI SICUREZZA | P.A. - AgID

Linee guida – La sicurezza nel procurement ICT | AgID

Nell'ambito delle procedure per l'approvvigionamento di **beni e servizi informatici**, RUP, responsabili della transizione al digitale, responsabili dell'organizzazione, pianificazione e sicurezza, nonché fornitori delle PP.AA.



DOVREBBERO RISPETTARE I SUGGERIMENTI DI AgID

Prendendo in considerazione i **principi privacy by design e by default** anche nell'ambito degli appalti pubblici (cons. 78 GDPR) fin dalla fase preliminare al procurement.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

144

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

Linee guida sulla formazione, gestione e conservazione dei documenti informatici | AgID

Le linee guida in commento, richiamano in più punti le Linee guida AgID in materia di misure minime di sicurezza ICT

Parere Garante Privacy

Il rinvio alle predette linee guida, nell'ambito dei requisiti di sicurezza cui sono tenuti i vari soggetti coinvolti nel trattamento, **non è di per sé sufficiente ad assicurare l'adozione di misure di sicurezza del trattamento adeguate**, in conformità al GDPR

Parere Garante Privacy

Occorre invece valutare, in concreto, i rischi che possono derivare, in particolare, dalla distruzione, dalla perdita, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

145

ANALIZZARE IL LIVELLO DI RISCHIO

Le **azioni di attacco** sono sempre più sofisticate, rese possibili dagli avanzamenti della tecnologia. L'assenza o l'inidoneità, spesso, di una **valutazione preventiva del rischio** (anche per mancanza di capacità specifiche e «orientate al rischio») rendono vulnerabili i sistemi operativi e gli applicativi nei quali circola un'**enorme quantità e varietà di dati**.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

146

ANALIZZARE IL LIVELLO DI RISCHIO

Le società che si occupano di sicurezza **danno evidenza con alcuni report** della dimensione del fenomeno comprensivo di attacchi informatici e data breaches, anche transfrontalieri.

**ENISA Threat Landscape
2020: Cyber Attacks
Becoming More
Sophisticated, Targeted,
Widespread and
Undetected**

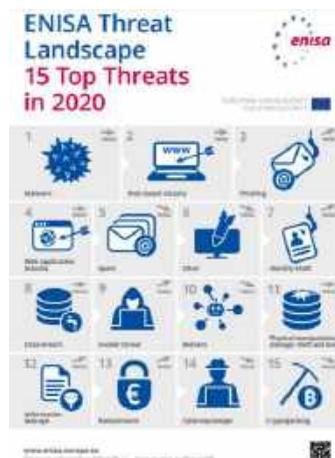
**From January 2019 to April
2020 Data breach
ENISA Threat Landscape**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

147

ANALIZZARE IL LIVELLO DI RISCHIO

**ENISA Threat
Landscape 2020:
Cyber Attacks
Becoming More
Sophisticated,
Targeted,
Widespread and
Undetected**



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

148

ANALIZZARE IL LIVELLO DI RISCHIO

I primi 15 rapporti sulle **minacce informatiche 2020** sono di natura tecnica e includono risultati, incidenti gravi, statistiche e altro ancora. I rapporti sulle minacce sono i seguenti:

1. Malware
2. Web-based Attacks
3. Phishing
4. Web Application Attacks
5. SPAM
6. Distributed Denial of Service (DDoS)
7. Identity Theft
8. **Data Breach**
9. Insider Threat
10. Botnets
11. Physical Manipulation, Damage, Theft and Loss
12. Information Leakage
13. Ransomware
14. Cyber Espionage
15. Cryptojacking

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

149

ANALIZZARE IL LIVELLO DI RISCHIO

RELAZIONE ANNUALE ENISA 2020, QUALCHE DATO

54% aumento del numero totale delle VIOLAZIONI a metà del 2019 rispetto al 2018.

71% delle violazioni dei dati sono state motivate da richieste di RISCATTO o per MOTIVI ECONOMICI.

Di queste, quasi il **25%** aveva obiettivi strategici a lungo termine (stato nazionale/spionaggio).

32% di violazioni dei dati coinvolgono attività di PHISHING.

Un rapporto suggerisce che il phishing è in cima alla lista dei principali motivi di violazione dei dati. Il rapporto menziona anche che la posta elettronica è il metodo di consegna principale del MALWARE (**94%**).

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

150



ANALIZZARE IL LIVELLO DI RISCHIO

RELAZIONE ANNUALE ENISA 2020, QUALCHE DATO

52% di violazioni dei dati coinvolti da HACKING.

Altre tecniche utilizzate sono gli **ATTACCHI SOCIALI (33%)**, il **MALWARE (28%)** **ERRORI (21%)**.

Dal 2016 l'hacking è stata la causa principale di violazioni dei dati nel settore sanitario. Nel corso del 2019 quasi **59%** delle violazioni segnalate sono stati causati da hacking.

70% di violazioni dei dati espongono E-MAIL (credenziali di accesso).

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

151



ANALIZZARE IL LIVELLO DI RISCHIO



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

152

ANALIZZARE IL LIVELLO DI RISCHIO

COSA SI EVINCE DAL REPORT DELL'ENISA?

- I costi relativi ad una violazione di dati personali si protraggono nel tempo
 - Da piccoli errori nella programmazione informatica della sicurezza dei sistemi possono derivare grandi violazioni
 - I data breach hanno un impatto e un costo maggiore sulle organizzazioni di minori dimensioni
 - L'obiettivo principale degli attacchi è la realizzazione di proventi illeciti
- I settori più colpiti sono...

Industry	Breaches	Small	Large	Outcomes
Accommodation	61	34	7	20
Administrative	17	6	6	5
Agriculture	2	2	0	0
Construction	11	7	3	1
Education	99	14	0	77
Entertainment	10	2	3	5
Finance	207	25	79	162
Healthcare	304	29	25	250
Information	155	20	18	117
Management	2	1	1	0
Manufacturing	87	10	22	50
Mining	15	2	5	8
Other services	54	6	5	49
Professional	157	34	10	113
Public	330	17	82	230
Real Estate	14	6	3	5
Retail	179	40	79	78
Trade	16	4	8	4
Transportation	36	3	9	24
Utilities	8	2	0	6
Unknown	289	0	109	180
Total	2,013	271	363	1,379

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

153

ANALIZZARE IL LIVELLO DI RISCHIO

COSA SI EVINCE DAL REPORT DELL'ENISA?

- I vettori sono:

A. E-MAIL/PHISHING



B. CLOUD/WEB APPLICATIONS

C. INSIDER THREAT



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

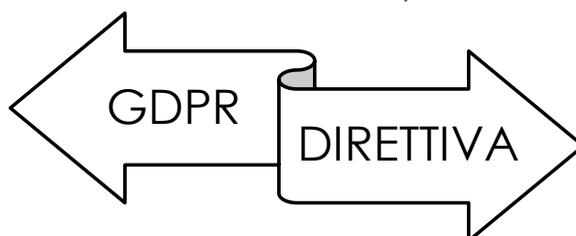
154



ANALIZZARE IL LIVELLO DI RISCHIO

Il GDPR suggerisce al titolare del trattamento un **approccio proattivo** rispetto alla sicurezza dei dati.

Rispetto alla Direttiva 95/46/CE è infatti basato sul **c.d. risk-based approach**, strettamente connesso al principio di accountability.



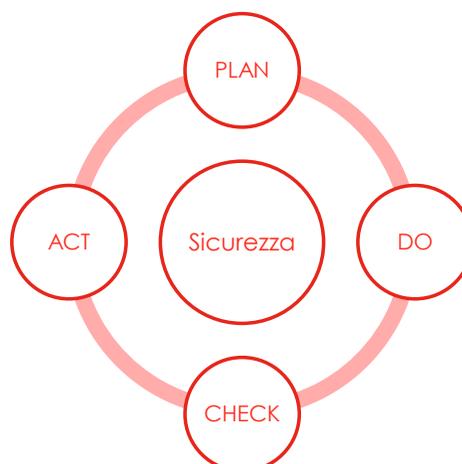
Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

155



ANALIZZARE IL LIVELLO DI RISCHIO

Per garantire il **«livello atteso» di sicurezza e protezione dei dati**, sarebbe utile adottare la sequenza di fasi tipica:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

156

ANALIZZARE IL LIVELLO DI RISCHIO

Con riguardo alla protezione dei dati personali, **le misure di sicurezza sono un asset competitivo**, e non devono essere viste come una spesa a fondo perduto o come un lusso incompatibile con le esigenze di economicità.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

157

ANALIZZARE IL LIVELLO DI RISCHIO

Quando si verifica un incidente informatico, il **budget** per la cybersecurity aumenta miracolosamente.



Nell'attacco che ha interessato il gruppo Piaggio si legge: «Nella giornata di ieri il soggetto responsabile del servizio CISO ha deciso di aggiornare il sistema di protezione del sistema informatico aziendale con l'obiettivo di potenziarlo».

I budget per la sicurezza informatica sono una questione complicata ma **è meno costoso prevenire gli attacchi informatici che riparare i danni quando si verificano.**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

158

ANALIZZARE IL LIVELLO DI RISCHIO

I Titolari del trattamento (o responsabili) che cercano di giustificare i loro budget per la sicurezza informatica hanno bisogno di modi per dimostrare il ritorno sull'investimento.

Una buona strategia è **presentare indicatori chiave di prestazione KPI**. Ad esempio:

1-Tentativi di intrusione: quante volte hanno tentato di violare le tue reti?

2-**Mean Time to Detect (MTTD)** : quanto tempo hai impiegato per venire a conoscenza di un potenziale incidente di sicurezza?

3-**Mean Time to Contain (MTTC)**: quanto tempo hai impiegato per contenere i vettori di attacco identificati?

4-**Mean Time to Resolve (MTTR)**: quanto tempo impieghi a rispondere a una minaccia una volta che ne sei a conoscenza?

ANALIZZARE IL LIVELLO DI RISCHIO

RACCOMANDAZIONI ENISA

- Considerare l'opportunità di **INVESTIRE IN STRUMENTI IBRIDI DI SICUREZZA** dei dati che si concentrino su un modello di responsabilità condivisa per gli ambienti cloud-based.
- Identificare e classificare i dati sensibili/personali e applicare **MISURE PER LA CIFRATURA** di tali dati in transito e a riposo.
- **AUMENTARE GLI INVESTIMENTI** in strumenti di rilevamento e di allerta e nella capacità di contenere e rispondere ad una violazione dei dati.
- Sviluppare e mantenere politiche forti che applichino **PASSWORD FORTI** (gestione delle password) e l'uso dell'autenticazione a più fattori.

ANALIZZARE IL LIVELLO DI RISCHIO

RACCOMANDAZIONI ENISA

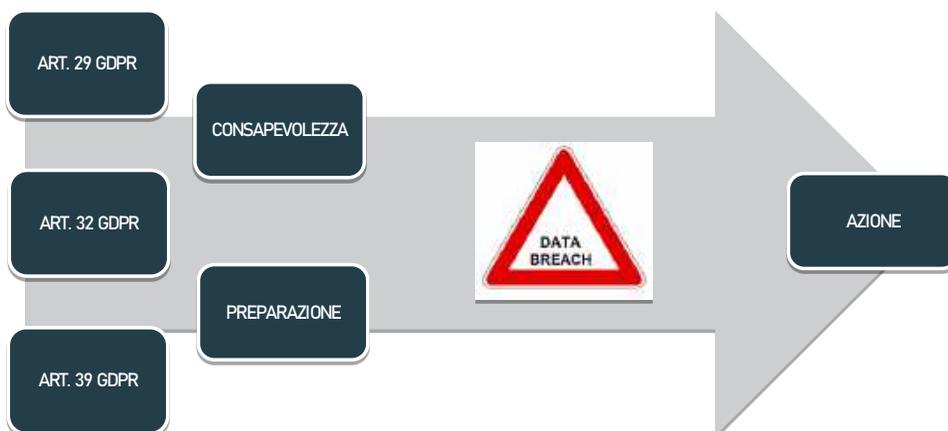
- **INVESTIRE E CREARE POLITICHE E PIANI** per coinvolgere i team di governance, di gestione del rischio e di conformità.
- Sviluppare e mantenere un piano di **SENSIBILIZZAZIONE ALLA SICUREZZA INFORMATICA**. Fornire scenari di formazione e simulazione per identificare le campagne di social engineering e phishing per il personale.
- Istituire e mantenere un **TEAM DI RISPOSTA AGLI INCIDENTI** e valutare frequentemente i piani di risposta agli incidenti.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

161

FORMAZIONE E SENSIBILIZZAZIONE IN AZIENDA



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

162

FORMAZIONE E SENSIBILIZZAZIONE IN AZIENDA



Art. 29 GDPR

*“Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali **non può trattare tali dati se non è istruito in tal senso** dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”*

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

163

FORMAZIONE E SENSIBILIZZAZIONE IN AZIENDA

Nel valutare l'adeguatezza delle misure adottate, l'ultimo paragrafo dell'**art. 32 GDPR** tiene conto di un parametro organizzativo: **le «istruzioni» preliminari che il titolare del trattamento deve impartire** a qualunque soggetto che, sotto l'autorità del titolare o del responsabile, possa aver accesso ai dati.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

164

FORMAZIONE E SENSIBILIZZAZIONE IN AZIENDA

Ai sensi dell'**art. 39 GDPR** il DPO deve curare *“la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo”*.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

165

VIOLAZIONE DEI DATI PERSONALI | DATA BREACH

“La violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione** non autorizzata o l'**accesso** ai dati personali trasmessi, conservati o comunque trattati”.



- **“violazione della riservatezza”**, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
- **“violazione dell'integrità”**, in caso di modifica non autorizzata o accidentale dei dati personali
- **“violazione della disponibilità”**, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

166

VIOLAZIONE DEI DATI PERSONALI | DATA BREACH

 <p>Perdita o furto di device mobili non criptati (usb, laptop, smartphone) che contengono dati personali</p>	 <p>Invio un file/email contenente dati personali al destinatario errato</p>
 <p>Invio di una email massiva a una lista di contatti nel campo "a:" o "cc:" invece che in "ccn:"</p>	 <p>Perdita o furto di documenti cartacei contenenti dati personali</p>
 <p>Attacchi informatici (malware, virus, criptolocker etc.) a sistemi contenenti dati personali</p>	 <p>Dati sanitari cartelle cliniche indisponibili per alcune ore a causa di attacco informatico o distacco elettrico</p>

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

167

VIOLAZIONE DEI DATI PERSONALI | DATA BREACH

IMPATTO NEI CONFRONTI DELL'INTERESSATO - (Considerando n. 85 GDPR)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

168

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

VIOLAZIONE DEI DATI PERSONALI | DATA BREACH

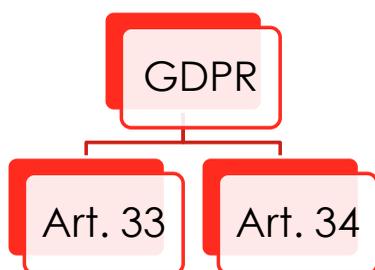
IMPATTO NEI CONFRONTI DELL'INTERESSATO - (Considerando n. 85 GDPR)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

169

VIOLAZIONE DEI DATI PERSONALI | DATA BREACH



Gli adempimenti relativi al data breach, **di cui agli artt. 33 e 34** del GDPR, rappresentano uno **strumento di tutela dell'interessato**, a presidio della liceità e correttezza del trattamento, **e**, nel contempo, di **garanzia della conformità dei titolari del trattamento** (e dei responsabili del trattamento) rispetto alla disciplina della protezione dei dati personali.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

170

COME GESTIRE UN DATA BREACH IN POCHE ORE

**IL DATA BREACH NON È UN
PROBLEMA SOLO TECNICO.**



COME GESTIRE GLI EFFETTI NEGATIVI
DEL DATA BREACH, SOPRATTUTTO SE
PUÒ IMPATTARE SIGNIFICATIVAMENTE
SU «DIRITTI E LIBERTÀ DELLE PERSONE
FISICHE»?

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

171

FORMAZIONE IN AZIENDA E LINEE GUIDA DATA BREACH

**Linee guida sulla notifica della violazione dei dati personali
3.10.2017 (agg. 6.2.2018)**

INCIDENTE DI SICUREZZA O DATA BREACH?



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

172

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

COME GESTIRE UN DATA BREACH IN POCHE ORE

È opportuno **verificare se** siano state messe in atto tutte le **misure tecnologiche e organizzative adeguate** di protezione per **stabilire immediatamente se** c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.

(Considerando 87 Reg. UE 2016/679)

COME GESTIRE UN DATA BREACH IN POCHE ORE

In concreto?

- Ruoli e responsabilità
- Procedure di violazione
- Reporting interno ed esterno
- Accordi di reporting con responsabili esterni
- Piani di intervento



COME GESTIRE UN DATA BREACH IN POCHE ORE

Ruoli e responsabilità

Incident Owner/Team Privacy

È il soggetto incaricato di gestire i Data Breach e gli Incidenti di sicurezza. Può coincidere con il responsabile tecnico dell'applicazione o del sistema coinvolto nel caso di incidenti collegati a sistemi informatici, con il responsabile dell'Area o con il Team di persone deputate a gestire tutti gli adempimenti privacy in azienda.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

175

COME GESTIRE UN DATA BREACH IN POCHE ORE

Ruoli e responsabilità

Il team di risposta è spesso composto da tecnici IT e di Sicurezza (IT e fisica); in alcuni casi possono essere coinvolti rappresentanti di altre funzioni di business a seconda della struttura organizzativa, per identificare le migliori azioni da mettere in atto per il ripristino dei prodotti/servizi minimizzando gli impatti sulla clientela.

Il contenimento dell'incidente consente di mettere in atto azioni immediate e tempestive nell'attesa di sviluppare una strategia risolutiva. Tali azioni possono essere di varia natura (es. spegnere un sistema, isolarlo dalla rete, disattivare specifiche funzioni ecc.) e sono tanto più efficaci quanto più sono già codificate all'interno dell'organizzazione.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

176

COME GESTIRE UN DATA BREACH IN POCHE ORE

Procedure di violazione

- avvisa immediatamente l'Incident Owner/Team privacy inviando una e-mail all'indirizzo privacy@_____;
- avvisa senza ritardo anche il referente della Tua area aziendale: deve conoscere il problema e supportarti/affiancarti nella sua gestione, anche organizzando/modificando la Tua attività lavorativa poiché tu sarai impegnato nella gestione di un possibile data breach;
- contatta telefonicamente l'Incident Owner/Team privacy per verificare che abbia letto la Tua email oppure, se qualcuno è assente o momentaneamente impegnato, contatta almeno uno dei membri del Team privacy ai recapiti indicati nel presente documento.

**Per l'autorizzato al
trattamento**

RICORDA: è importante intervenire tempestivamente, per cui non perdere tempo e metfifi in contatto con il referente a te più vicino!

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

177

COME GESTIRE UN DATA BREACH IN POCHE ORE

Procedure di violazione

- A seguito della segnalazione di un presunto data breach, l'Incident Owner/Team privacy deve immediatamente contattare gli altri membri del team per farsi aiutare nella gestione del presunto data breach.
- L'Incident Owner o i membri del Team privacy dovranno mettersi in contatto con l'autore della segnalazione per stabilire se sia effettivamente accaduto un data breach e se sia necessaria un'indagine più approfondita dell'accaduto. A tale scopo, dovranno esaminare l'allegato compilato dall'autore della segnalazione, eventualmente aiutando quest'ultimo a completare tale allegato nelle parti rimaste ancora incomplete.

**Per l'Incident
owner/Team
privacy**

RICORDA: È necessario chiedere (e pretendere) sempre informazioni precise ed un riscontro entro e non oltre le successive 24 ore, dato che la notifica all'Autorità Garante di un data breach deve avvenire entro 72 ore dalla scoperta dell'evento: c'è poco tempo, per cui non sono ammessi ritardi.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

178



COME GESTIRE UN DATA BREACH IN POCHE ORE

Reporting interno ed esterno

CONTENUTO PARAGRAFO	NUM.
1. Obiettivo generale del documento: definire le procedure da seguire in caso di violazione di dati personali, con particolare riferimento alle attività di reporting interno ed esterno.	1
2. Campo di applicazione: il presente documento si applica a tutti i dipendenti, collaboratori, consulenti e fornitori dell'azienda.	2
3. Definizione di Data Breach: qualsiasi incidente che comporti la perdita, l'accesso non autorizzato, la divulgazione o l'alterazione non autorizzata di dati personali.	3
4. Procedure di reporting interno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla segnalazione iniziale alla valutazione dell'incidente e all'adozione delle misure di contenimento.	4
5. Procedure di reporting esterno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla valutazione dell'incidente alla comunicazione alle autorità competenti e all'interessato.	5
6. Misure di contenimento e recupero: descrizione delle attività da svolgere per limitare l'impatto della violazione e ripristinare la sicurezza dei dati personali.	6
7. Misure di prevenzione: descrizione delle attività da svolgere per prevenire il verificarsi di future violazioni di dati personali.	7
8. Note finali: informazioni aggiuntive e contatti di riferimento.	8

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.



COME GESTIRE UN DATA BREACH IN POCHE ORE

CONTENUTO PARAGRAFO	NUM.
1. Obiettivo generale del documento: definire le procedure da seguire in caso di violazione di dati personali, con particolare riferimento alle attività di reporting interno ed esterno.	1
2. Campo di applicazione: il presente documento si applica a tutti i dipendenti, collaboratori, consulenti e fornitori dell'azienda.	2
3. Definizione di Data Breach: qualsiasi incidente che comporti la perdita, l'accesso non autorizzato, la divulgazione o l'alterazione non autorizzata di dati personali.	3
4. Procedure di reporting interno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla segnalazione iniziale alla valutazione dell'incidente e all'adozione delle misure di contenimento.	4
5. Procedure di reporting esterno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla valutazione dell'incidente alla comunicazione alle autorità competenti e all'interessato.	5
6. Misure di contenimento e recupero: descrizione delle attività da svolgere per limitare l'impatto della violazione e ripristinare la sicurezza dei dati personali.	6
7. Misure di prevenzione: descrizione delle attività da svolgere per prevenire il verificarsi di future violazioni di dati personali.	7
8. Note finali: informazioni aggiuntive e contatti di riferimento.	8

CONTENUTO PARAGRAFO	NUM.
1. Obiettivo generale del documento: definire le procedure da seguire in caso di violazione di dati personali, con particolare riferimento alle attività di reporting interno ed esterno.	1
2. Campo di applicazione: il presente documento si applica a tutti i dipendenti, collaboratori, consulenti e fornitori dell'azienda.	2
3. Definizione di Data Breach: qualsiasi incidente che comporti la perdita, l'accesso non autorizzato, la divulgazione o l'alterazione non autorizzata di dati personali.	3
4. Procedure di reporting interno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla segnalazione iniziale alla valutazione dell'incidente e all'adozione delle misure di contenimento.	4
5. Procedure di reporting esterno: descrizione delle attività da svolgere in caso di violazione di dati personali, dalla valutazione dell'incidente alla comunicazione alle autorità competenti e all'interessato.	5
6. Misure di contenimento e recupero: descrizione delle attività da svolgere per limitare l'impatto della violazione e ripristinare la sicurezza dei dati personali.	6
7. Misure di prevenzione: descrizione delle attività da svolgere per prevenire il verificarsi di future violazioni di dati personali.	7
8. Note finali: informazioni aggiuntive e contatti di riferimento.	8

17. In caso di violazione di dati personali, il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per porre fine alla violazione e limitare al massimo il danno, nonché valutare se è opportuno notificare la violazione all'autorità di controllo e all'interessato.	17
18. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per prevenire il verificarsi di future violazioni di dati personali.	18
19. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali.	19
20. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la riservatezza dei dati personali.	20
21. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire l'integrità dei dati personali.	21
22. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la disponibilità dei dati personali.	22
23. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la resilienza dei dati personali.	23
24. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali.	24
25. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la riservatezza dei dati personali.	25
26. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire l'integrità dei dati personali.	26
27. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la disponibilità dei dati personali.	27
28. Il titolare del trattamento deve adottare le misure tecniche e organizzative adeguate per garantire la resilienza dei dati personali.	28

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

COME GESTIRE UN DATA BREACH IN POCHE ORE

Accordi di reporting con responsabili esterni

CLAUSOLA «Violazione dei dati»

Se dovesse venire a conoscenza di una violazione dei dati personali (Data Breach), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

Il Responsabile deve coadiuvare il Titolare del trattamento nella redazione di specifiche procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative procedure di risposta attraverso l'elaborazione di una specifica policy.

Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

COME GESTIRE UN DATA BREACH IN POCHE ORE

Accordi di reporting con responsabili esterni

CLAUSOLA «Violazione dei dati»

Nello specifico dovranno essere documentati:

- a) la natura della violazione dei dati personali compresi,;
- b) il nome e i dati di contatto del DPO (se nominato) o di altro punto di contatto;
- c) la descrizione delle probabili conseguenze della violazione dei dati personali;
- d) la descrizioni delle misure adottate o di cui si propone l'adozione.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (Data breach) prevista dall'art. 33 comma 3 del GDPR.

COME GESTIRE UN DATA BREACH IN POCHE ORE



Il Responsabile del trattamento → **non deve valutare la probabilità di rischio** derivante dalla violazione prima di notificarla al titolare del trattamento; spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione.

Deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento.

COME GESTIRE UN DATA BREACH IN POCHE ORE

Piani di intervento

RESPOND: definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le categorie all'interno di questa funzione sono:

Response Planning
Communications
Analysis
Mitigation
Improvements



COME GESTIRE UN DATA BREACH IN POCHE ORE

Piani di intervento

Rapporto finale:	descrizione obiettiva dell'incidente
	controlli esistenti al momento dell'incidente
	elenco delle misure di risposta efficaci
	ripetibilità dell'incidente in circostanze simili
	metodi di rilevazione utilizzati
	composizione team di governance/risposta e comunicazioni intervenute

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

185

COME GESTIRE UN DATA BREACH IN POCHE ORE



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

186

COME NOTIFICARE E COMUNICARE UN DATA BREACH

Articolo 33

72 ORE

- **Notifica del Data Breach all'Autorità di Controllo 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.
- Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa è corredata dei motivi del ritardo.

COME NOTIFICARE E COMUNICARE UN DATA BREACH

La notifica deve:

- 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
- 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
- Descrivere le probabili **conseguenze** della violazione dei dati personali
- 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, per attenuarne i possibili effetti negativi.

COME NOTIFICARE E COMUNICARE UN DATA BREACH

Art. 34 - Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali presenta un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato **senza ingiustificato ritardo**.



La comunicazione all'interessato descrive con un **linguaggio semplice e chiaro la natura della violazione**.

Quando vi è rischio?

quando la **violazione può comportare un danno fisico, materiale o immateriale** per le persone fisiche i cui dati sono stati violati

COME NOTIFICARE E COMUNICARE UN DATA BREACH

Metodi trasparenti di comunicazione sono:

Sì | La messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa.

No | Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato.

COME NOTIFICARE E COMUNICARE UN DATA BREACH

Il ruolo del DPO nel Data Breach

Ai sensi dell'art. 38 GDPR, il Titolare e il Responsabile assicurano che il DPO sia **“tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali”**.

Il DPO deve consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (linee guida 3.1).



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

191

IL REGISTRO DELLE VIOLAZIONI

Il Titolare del trattamento **documenta** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Progressione	Stato	DPO	Data violazione	Stato violazione
1	Chiuso	Albert Belloni	20/04/2018	Chiuso
2	Chiuso	Albert Belloni	18/07/2018	Chiuso
3	Aperto	Albert Belloni	20/04/18	Aperto

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

192

VIOLAZIONE DEI DATI PERSONALI

Affronta la violazione dei dati personali con:

- Procedura interna sulla violazione dei dati personali
- Scadenziario violazione
- Valutazione rischio evento
- Registrazione della violazione

REGISTRO VIOLAZIONI DEI DATI PERSONALI

Privacy Encoder

<https://www.privacyencoder.com/>

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

193

CASE HISTORY

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/ raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

194

CASE HISTORY

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
<p>Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati.</p> <p>Il titolare del trattamento ha clienti in un solo Stato membro.</p>	<p>Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.</p>	<p>Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.</p>	

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

195

CASE HISTORY

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
<p>Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.</p>	<p>Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).</p>	<p>Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.</p>	<p>La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.</p>

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

196

CASE HISTORY



Malfunzionamenti del sito che hanno comportato la possibilità di accedere a **informazioni riguardanti altre persone**, tra cui nome e cognome e documenti personali.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

197

CASE HISTORY

Provvedimento sui data breach INPS: comunicazione agli interessati coinvolti - 14 maggio 2020 [9344061]

INPS | “Chi ha consultato avrebbe avuto uno scarso interesse a conoscere i dati visualizzati e dunque uno **scarso impatto sulla sfera personale degli interessati**. Allo stesso tempo, l'impossibilità di fare ricerche mirate, la casualità e l'evidenza che chi ha accaduto ha una residenza distante dagli interessati, denotano una scarsa probabilità che i dati siano stati visualizzati da soggetti che potevano avere interesse ad incidere sulla sfera personale dei soggetti coinvolti. Sulla base di tali valutazioni di rischio, l'Istituto ritiene che **la violazione non sia tale da rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche**”

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

198

CASE HISTORY



Violazioni dei dati personali suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche → **comunicazione agli interessati ex art. 34, par. 1 GDPR obbligatoria** in considerazione dei seguenti fattori:



1. Aspetti di carattere generale

2. violazione dei dati personali determinata dal caching delle informazioni personali presenti nelle pagine del portale "www.inps.it":

3. violazione dei dati personali determinata dall'errata configurazione del sistema di autorizzazione della procedura Bonus Baby Sitting

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

Art. 35 GDPR e linee guida WP29 | 4 aprile 2017
DPIA: Valutazione d'impatto sulla protezione dei dati



VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

Rischio	Misure
Non elevato	Adozione di misure idonee
Elevato	Prima dell'adozione delle misure idonee e del trattamento è necessario effettuare un DPIA
Elevato senza possibilità di attenuare il rischio	Consultazione del Garante Privacy

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

201

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

Quando?

La valutazione d'impatto sulla protezione dei dati è richiesta, **PRIMA di procedere al trattamento, in caso di:**

- a) Valutazione **sistematica e globale** di aspetti personali basata su **trattamento automatizzato**, compresa la **profilazione**
- b) **Trattamento, su larga scala** di **categorie particolari** di dati o di dati relativi a **condanne penali**
- c) **Sorveglianza sistematica** su larga scala di una zona accessibile al pubblico.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

202

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

PUNTO 4 ART. 35

prevede che l'**Autorità di controllo** (DPA) **rediga e renda pubblico un elenco** delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati e comunica tali elenchi all'EDPB.

L'Italia lo ha pubblicato a Novembre 2018

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

Il titolare del trattamento può ritenere che quando un trattamento soddisfa **anche uno solo** di questi criteri precedentemente indicati, tenuto conto delle circostanze del caso, sia necessario condurre una DPIA.



VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

205

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

In che cosa consiste?

La valutazione contiene almeno:

- Una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, l'**interesse legittimo** perseguito dal titolare del trattamento
- una **valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità
- una **valutazione dei rischi** per i diritti e le libertà degli interessati di cui al paragrafo 1
- le **misure previste per affrontare i rischi**, includendo le **garanzie**, le **misure di sicurezza** e i **meccanismi per garantire la protezione dei dati personali** e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

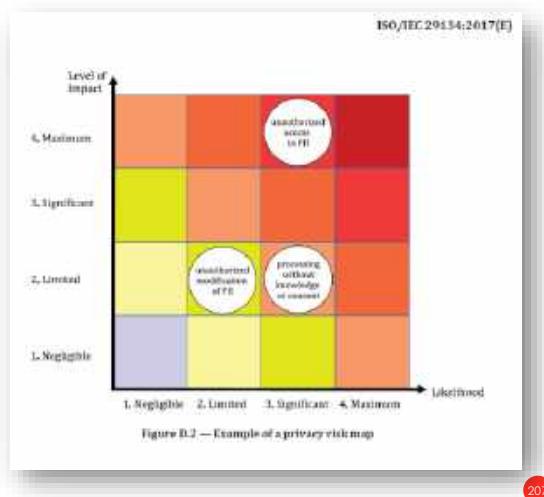
Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

206

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

Quale metodologia utilizzare ?

1. Una norma internazionale che fornisce orientamenti in merito alle metodologie utilizzate per la realizzazione di una valutazione d'impatto sulla protezione dei dati (**ISO/IEC 29134**)



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA

2. Un **modello adottato da una Autorità Garante Nazionale** ed elencati nell'allegato a) della linea Guida del WP 29

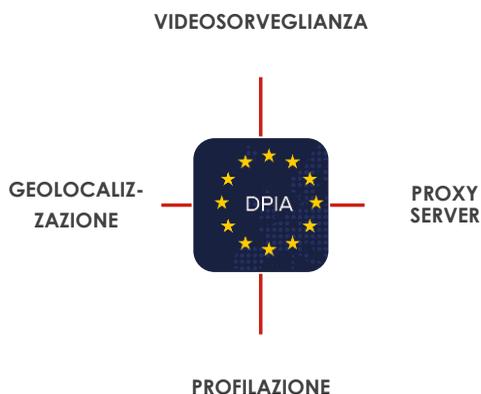
<https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

208

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | DPIA



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

209

IL DPO – RPD NELLA PUBBLICA AMMINISTRAZIONE

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

210

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

DESIGNAZIONE del RESPONSABILE della PROTEZIONE dei DATI (Art. 37, c. 5 GDPR)

«Il responsabile della protezione dei dati è designato in funzione delle **qualità professionali**, in particolare della **conoscenza specialistica della normativa** e delle **prassi in materia di protezione dei dati**, e della capacità di assolvere i compiti di cui all'articolo 39»

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento.

Per **esempio**, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Qualifica nella P.A. - FAQ

Il GDPR non fornisce specifiche indicazioni al riguardo.



- È opportuno, in primo luogo, valutare se il complesso dei compiti assegnati al DPO - aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) - siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale.
- Quindi se interno, sarebbe in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un **dirigente** ovvero a un **funzionario di alta professionalità**, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD



Art. 39 – Compiti del DPO – RPD

Informare/fornire consulenza al Titolare, al Responsabile del Trattamento e ai dipendenti che trattano dati personali;

Sorvegliare l'osservanza del Regolamento/altre disposizioni dell'UE sulla protezione dei dati e delle politiche adottate in materia di protezione dei dati;

Fornire un parere, ove richiesto, su eventuali **DPIA** effettuate dal Titolare;

Cooperare/fungere da punto di contatto con l'Autorità di controllo.

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Art. 38 - Posizione del DPO | RPD

- Deve essere **adeguatamente coinvolto** in tutte le questioni sulla protezione dei dati personali;
- Deve avere le **risorse necessarie** per adempiere ai compiti previsti dall'art. 39 GDPR e deve mantenere la propria **conoscenza specialistica**;
- NON deve **ricevere istruzioni** per quanto riguarda l'esecuzione dei suoi compiti;
- NON può **essere rimosso o penalizzato** dal Titolare del trattamento (o dal Responsabile del trattamento) per l'adempimento dei propri compiti.
- **Riferisce** direttamente al **verice gerarchico** del titolare del trattamento o del responsabile del trattamento;
- È tenuto al **segreto/riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri;
- Può svolgere **altri compiti e funzioni**.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

215

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

- Nel Manuale RPD|DPO elaborato per il programma «T4DATA» finanziato dall'UE vengono precisati in 15 punti i **compiti del RPD|DPO operante nel settore pubblico e parapubblico**

Compiti

1. Creazione di un registro delle attività di trattamento di dati personali
2. Riesame delle attività di trattamento di dati personali
3. Valutazione dei rischi posti dalle attività di trattamento di dati personali

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

216

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Compiti

4. Gestione dei trattamenti che possono comportare un «rischio elevato»: DPIA
5. Ripetizione dei Compiti 1 – 4 su base continuativa
6. Gestione delle violazioni di dati personali
7. Compiti di indagine (compresa la gestione dei reclami interni ed esterni)
8. Funzioni di consulenza – aspetti generali

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

217

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Compiti

9. Sostegno e promozione dei principi di «Protezione dei dati fin dalla progettazione e la Protezione dei dati per impostazione predefinita» (Data protection by Design & Default)
10. Consulenza e monitoraggio della conformità delle politiche di protezione dei dati, dei contratti di contitolarità, titolare-titolare e titolare-responsabile, norme vincolanti d'impresa e clausole per il trasferimento di dati
11. Coinvolgimento nei codici di condotta e nelle certificazioni

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

218

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Compiti

12. Cooperazione con l'Autorità di protezione dati

13. Gestione di richieste e reclami dell'interessato

14. Compiti di informazione e di sensibilizzazione
interna ed esterna

15. Pianificazione e riesame delle attività del RPD

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Quando la GDF bussa alla porta della società...

- GDF arriva SENZA ANNUNCIARSI
- DURATA: la stabiliscono all'inizio dell'ispezione (3gg con maggiorazione in caso di identificazione di problematiche da approfondire)
- Chiedono PRESENZA del TITOLARE DEL TRATTAMENTO (nella persona dell'AD o del PROCURATORE DELEGATO ai rapporti con le autorità esterne) – produrre copia della procura
- GDF manifesta LO SCOPO DELL'ISPEZIONE (es. *acquisire ogni utile informazione e documento con riferimento a trattamenti di dati personali per il rilascio di Fidelity Card*)
- GDF rendono edotta la parte della possibilità di AVVALERSI DI ALTRE PERSONE DI FIDUCIA ad assistere in maniera idonea nell'attività ispettiva
- GDF rende edotti i presenti delle RESPONSABILITÀ PENALI, DELLE SANZIONI e dell'obbligo di dimostrarsi collaborativi

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Cosa fa il DPO durante l'ispezione?

- Raggiunge il Titolare nel più breve tempo possibile (tale aspetto viene verbalizzato)
- Può intervenire su qualsiasi richiesta di informazioni/documentazione posta dalla GDF ai presenti
 - Referenti preparati ad affrontare l'ispezione, conoscendo il loro business di appartenenza anche dal punto di vista privacy
 - Prima dell'avvio dell'ispezione briefing di confronto DPO/referenti

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

221

RESPONSABILE DELLA PROTEZIONE DEI DATI | DPO - RPD

Cosa fa il DPO durante l'ispezione?

- Non rilasciare false dichiarazioni
- Approccio collaborativo con la GDF, mediando tra l'autorità e gli intervistati
- Sottoscrive il/i verbale/i alla chiusura della/e giornata/e di ispezione e vidima le singola pagine, avendo cura di rileggerlo in maniera approfondita e presentando eventuali osservazioni o chiedendo modifiche

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

222

IL SISTEMA SANZIONATORIO

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

223

SISTEMA SANZIONATORIO

In caso di violazioni in tema data protection:

Richieste Risarcimento	Tribunale Civile
Sanzioni amministrative	Art. 83 GDPR Garante
Sanzioni penali	Singolo Stato membro Giudice Penale



DIRITTO AL RISARCIMENTO E RESPONSABILITÀ

Art. 82 GDPR



- Chiunque subisca un **danno materiale o immateriale** causato da una **violazione del Regolamento** ha il diritto di ottenere il **risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento.
- Il **Responsabile del trattamento** risponde per:
 - inosservanza obblighi imposti dal GDPR;
 - non conformità/contrarietà della condotta rispetto alle istruzioni del Titolare del trattamento.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

225

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ

segue..



- Il Titolare del trattamento o il Responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile → **inversione onere della prova.**
- **Responsabilità in solido** in caso di più soggetti (salvo accordo fra le parti) → **diritto di «reclamo»** dagli altri titolari o co-responsabili in caso di pagamento della sanzione per intero.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

226

SANZIONI AMMINISTRATIVE E PECUNIARIE

Art. 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

227

SANZIONI AMMINISTRATIVE E PECUNIARIE

Le DPA per irrogare **SANZIONI** devono tener conto:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

228

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

SANZIONI AMMINISTRATIVE E PECUNIARIE

Nel caso di **Pubbliche Amministrazioni** spetta agli Stati determinare se e in che misura debbano essere sanzionate



N.B. → se in relazione allo stesso trattamento o a trattamenti collegati un titolare o un responsabile del trattamento viola **con dolo o colpa** varie disposizioni del Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la **violazione più grave (ART. 83, c. 3 GDPR)**.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

229

SANZIONI AMMINISTRATIVE E PECUNIARIE

NOTA BENE

Ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad **autorità pubbliche e organismi pubblici** istituiti in tale Stato membro.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

230

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

SANZIONI AMMINISTRATIVE E PECUNIARIE



- 09 luglio 2020: il Garante sanziona l'Istituto Comprensivo Statale Crucoli Torretta per **diffusione** di dati personali (anche particolari) di studenti attraverso il sito web istituzionale.
- 09 luglio 2020: il Garante sanziona il Comune di Baronissi per **diffusione** di dati personali attraverso il sito web istituzionale.
- 02 luglio 2020: il Garante sanziona l'Istituto comprensivo statale di Uggiano la Chiesa per l'**affissione** all'ingresso, di taluni elenchi contenenti dati personali degli studenti (minori).

In tutti e tre i casi **SANZIONE: 2.000,00 EURO**

SANZIONI AMMINISTRATIVE E PECUNIARIE



- 2 luglio 2020: Il Garante sanziona l'Istituto Nazionale della Previdenza Sociale - Direzione Provinciale di Brescia per **mancato riscontro all'istanza** di accesso ai dati (su invito dell'Autorità Garante).

SANZIONE: 5.000,00 EURO

- 23 gennaio 2020: Il Garante sanziona l'Azienda Ospedaliero Universitaria Integrata di Verona, su notifica della stessa, per non aver adottato adeguate misure per prevenire l'**accesso** a dati personali (anche particolari) **a soggetti non autorizzati**.

SANZIONE: 30.000,00 EURO

ALTRE SANZIONI

Oltre alle sanzioni amministrative le DPA - in aggiunta o in luogo delle stesse – possono
(Art. 58):

- rivolgere **avvertimenti** al Titolare /Responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente Regolamento
- rivolgere **ammonimenti** al Titolare /Responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente Regolamento



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

233

ALTRE SANZIONI

- **ingiungere** al Titolare del trattamento o al Responsabile del trattamento **di soddisfare le richieste dell'interessato** di esercitare i diritti loro derivanti dal presente Regolamento
- **ingiungere** al Titolare del trattamento o al Responsabile del trattamento **di conformare i trattamenti alle disposizioni del presente Regolamento**, se del caso, in una determinata maniera ed entro un determinato termine
- **ingiungere** al Titolare del trattamento di **comunicare all'interessato una violazione dei dati personali**
- **imporre** una **limitazione provvisoria o definitiva** al trattamento, incluso il divieto di trattamento

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

234

ALTRE SANZIONI

- **ordinare la rettifica, la cancellazione** di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19
 - **revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- **ordinare la sospensione dei flussi di dati** verso un destinatario in un Paese terzo o un'organizzazione internazionale.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

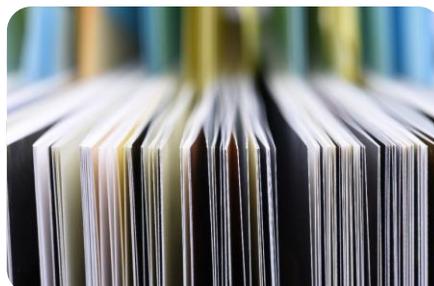
235

REGISTRO DELLE SANZIONI

Ogni Autorità di controllo promuove, insieme al comitato europeo per la protezione dei dati un **registro di sanzioni e violazioni**.

Tale registro deve contenere:

- tutti gli avvertimenti
- le sanzioni
- la risoluzione delle violazioni



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

236

RESPONSABILITÀ PENALE | CODICE PRIVACY 196/03

Vengono penalmente sanzionati:

- Il trattamento illecito di dati personali - Art. 167
- La comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala – Art.167bis
- L'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala – Art.167ter
 - Le false dichiarazioni rese al Garante - Art. 168
- L'inosservanza dei provvedimenti del Garante – Art.170
 - La violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori – Art. 171



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

237

TUTELA INTERESSATO

**Forme di tutela
interessato**

Reclamo al Garante

Ricorso Autorità Giudiziaria

Segnalazione al Garante

Reclamo ex art. 77 del Regolamento (UE) 2016/679

Il/La sottoscritto/a....., nato/a ail residente in..... CF....., il/la quale ai fini del presente procedimento dichiara di voler ricevere eventuali comunicazioni al seguente indirizzo (fisico o di posta elettronica.....) espone quanto segue:

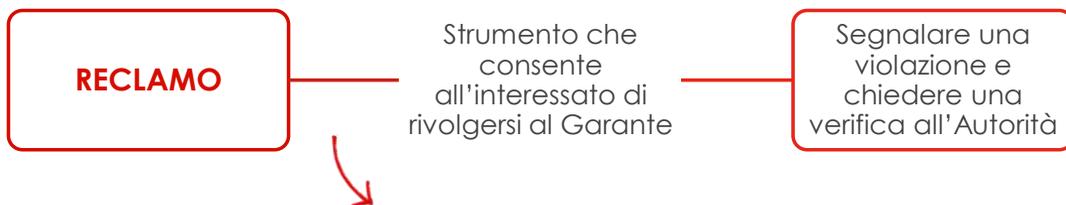


**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

238

RECLAMO



Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro → procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato.

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9041356>

SEGNALAZIONE



Art. 144 - Segnalazioni

Chiunque può rivolgere una **segnalazione** che il Garante può valutare *anche ai fini dell'emanazione dei provvedimenti* di cui all'articolo 58 del Regolamento (es. ingiunzione al Titolare | accesso ai dati ecc.)

I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio.

PROVVEDIMENTI PRIVACY (cenni): Videosorveglianza e Biometria

IL GDPR NELLA PUBBLICA AMMINISTRAZIONE,
CRITICITÀ E SOLUZIONI

241

VIDEOSORVEGLIANZA | PROVVEDIMENTO 8 APRILE 2010



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

Con il **provvedimento 8 aprile 2010 in tema di videosorveglianza**, Il Garante per la protezione dei dati personali ha chiarito i principi ed i precetti generali applicabili al trattamento di dati personali mediante l'utilizzo di impianti di videosorveglianza nei vari settori pubblici e privati.

242

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

VIDEOSORVEGLIANZA | PRINCIPI GENERALI

Principi generali – applicabili sia ad enti pubblici che privati

Liceità

Necessità

Proporzionalità

Finalità



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

243

VIDEOSORVEGLIANZA | PRINCIPI GENERALI

Liceità → Il trattamento deve fondarsi sui presupposti di liceità / basi giuridiche del trattamento ai sensi dell'art.6 del GDPR



Tutte le basi giuridiche di cui all'art. 6 GDPR possono costituire un legittimo fondamento al trattamento dei dati

Nella pratica, le più usate sono:

- la **legge** – Art. 6 lett. c) GDPR si applica laddove sia la stessa legge nazionale a prevedere l'obbligo di videosorveglianza;
- Il **legittimo interesse** – Art. 6 lett. f) GDPR;
- L'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento – Art. 6 lett. e) GDPR

In casi eccezionali, il **consenso** – Art. 6 lett. a) GDPR

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

244

VIDEOSORVEGLIANZA | PRINCIPI GENERALI



I dati personali devono essere **adeguati**, **pertinenti** e **limitati** in relazione alle finalità per i quali sono trattati (**minimizzazione dei dati**), ai sensi dell'Art. 5, lett. c), GDPR.

Prima di installare un sistema di videosorveglianza il titolare dovrebbe verificare che tale misura è proporzionata alla finalità perseguita.

Extrema ratio: valutare l'adozione di misure alternative.

VIDEOSORVEGLIANZA | PRINCIPI GENERALI

Nel rispetto del principio di **minimizzazione dei dati**
l'**EDPB suggerisce:**

- adozione di misure di sicurezza alternative quali ad es. assunzione di personale di vigilanza

oppure

- valutare dove e quando le telecamere di sorveglianza sono strettamente necessarie

VIDEOSORVEGLIANZA | SOGGETTI PUBBLICI

Ai sensi del Provvedimento in materia di videosorveglianza, i **soggetti pubblici** possono effettuare attività di videosorveglianza solo ed esclusivamente per lo svolgimento delle proprie **funzioni istituzionali** che devono individuare ed esplicitare con esattezza.

Gli impianti possono essere destinati ad esempio per:

Sicurezza urbana

Alla luce del D.L. 20 Febbraio 2017, N. 14, è necessario valutare se la finalità istituzionale perseguita sia **espressamente prevista dalla legge**.

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

INFORMATIVA DI PRIMO LIVELLO

Gli interessati devono essere informati con speciale segnaletica informativa **prima del raggio di azione** delle telecamere, in maniera ben visibile, anche in orario notturno.

Segnaletica «VIGNETTA» differente in base alla **registrazione** o alla **mera rilevazione in modalità live** delle immagini.



VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

**Quali sono gli elementi
costitutivi della vignetta?**



Titolare del trattamento – **DPO** ove applicabile

Finalità di trattamento

Modalità di funzionamento
dell'impianto

(registrazione o mera rilevazione in
modalità live)

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

249

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

Visualizzazione da parte di terzi

SE ISTITUTO DI VIGILANZA:

- Nomina responsabile art. 28 GDPR per visualizzazione delle immagini;
- File di Log degli accessi.



SE FORZE DELL'ORDINE:

- Vignetta specifica.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

250

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

VIDEOSORVEGLIANZA | OBBLIGHI DEL TITOLARE

INFORMATIVA DI SECONDO LIVELLO

Informativa dipendenti

in forma estesa (ex Art. 13
GDPR, con riferimenti all'Art. 4
Legge 300/70 – Jobs Act)

Informativa visitatori/clienti

in forma estesa (ex Art. 13
GDPR)

Devono essere rese
disponibili in un **luogo
facilmente accessibile** agli
interessati (es. reception o
sito dell'organizzazione).



In ogni caso, **deve essere
possibile accedere alle
informazioni di secondo
livello senza accedere
all'area videosorvegliata.**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

251

VIDEOSORVEGLIANZA | TEMPI DI CONSERVAZIONE

Principio di proporzionalità: le
immagini possono essere
conservate solo per il tempo
strettamente necessario al
perseguimento della finalità
prefissata.

Massimo **24 ore dalla registrazione**,
fatte salve esigenze di ulteriore
conservazione in relazione a festività o
chiusura degli esercizi, nonché i casi in
cui si debba aderire a specifiche
richieste investigative delle Autorità
giudiziarie.

**Solo in alcuni casi, per esigenze
tecniche o di particolare rischiosità
dell'attività svolta, è consentita la
conservazione per un periodo superiore.**

Andranno predisposte misure tecniche
od organizzative per la **cancellazione,
anche in forma automatica**, delle
registrazioni, allo scadere del termine di
legge: sovrascrittura, cancellazione.



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

252

VIDEOSORVEGLIANZA | TEMPI DI CONSERVAZIONE

*Prima del GDPR → qualora si intendeva procedere ad un allungamento dei tempi di conservazione per un periodo superiore alla settimana doveva essere sottoposta una **richiesta di verifica preliminare al Garante***

In tal senso il Garante si è più volte pronunciato positivamente in seguito alla richiesta di adozione di

- allungamento dei tempi di conservazione (fino anche a 90 giorni)
- sistemi di videosorveglianza c.d. «intelligenti»

per specifici settori quali Musei statali, aree archeologiche, opere artistiche e religiose.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

253

VIDEOSORVEGLIANZA | TEMPI DI CONSERVAZIONE

Nella verifica preliminare richiesta dalla Soprintendenza per i beni archeologici delle Marche - [doc. web n. 2138277] il Garante

innanzitutto richiama il D.L. 14 novembre 1992 n. 433 convertito con modificazioni dalla L. 14 gennaio 1993 n. 4

secondo cui con riferimento ai musei statali è autorizzata l'installazione di impianti audiovisivi per il controllo continuativo ed ininterrotto dei beni culturali esposti con finalità di prevenzione e di tutela da azioni criminose e danneggiamenti

autorizza l'allungamento dei tempi di conservazione – per un periodo non superiore ai 30 giorni – considerate **le specifiche esigenze di sicurezza e di tutela del patrimonio artistico e museale** con particolare riferimento al **traffugamento delle opere d'arte di interesse storico-artistico.**

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

254

VIDEOSORVEGLIANZA | SISTEMI C.D. «INTELLIGENTI»

Il Garante – a seguito di richieste di verifica preliminare – ha inoltre autorizzato l'adozione di **sistemi di videosorveglianza c.d. «intelligenti»**



sistemi che non si limitano a riprendere e registrare le immagini ma che sono in grado di *rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli*

per finalità di sicurezza urbana valutata l'esigenza di tutela di siti monumentali e istituzionali e di tutela del patrimonio artistico

VIDEOSORVEGLIANZA | LUOGHI DI LAVORO

Non vi deve essere attività di **controllo illecita sulle attività del lavoratore** (cfr. artt. 4 – 8 Legge 300/70 - Statuto dei Lavoratori)

Divieto di:

- Riprendere **lettori badge** per timbrature del personale o luoghi da cui si potrebbe evincere la diligenza del lavoratore in genere (postazione del lavoratore)
- Utilizzo di impianti audiovisivi e di altri strumenti che abbiano quale **finalità unica ed esclusiva il controllo a distanza** del lavoratore (Art. 4 Legge 300/70 – Jobs Act D.lgs. 14 settembre 2015, n. 151)



VIDEOSORVEGLIANZA | LUOGHI DI LAVORO

Comma 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori **possono essere impiegati esclusivamente per esigenze:**

- organizzative e produttive
- per la sicurezza del lavoro
- e per la tutela del patrimonio aziendale

E

possono essere installati **previo accordo collettivo** stipulato dalla rappresentanza sindacale unitaria (**RSU**) o dalle rappresentanze sindacali aziendali (**RSA**) o associazioni sindacali comparativamente più rappresentative sul piano nazionale

VIDEOSORVEGLIANZA | LUOGHI DI LAVORO

Se non presenti:

previa autorizzazione della sede territoriale dell'Ispettorato Nazionale del Lavoro (ITL) ovvero - in caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali - della sede centrale dell'Ispettorato Nazionale del Lavoro.



VIDEOSORVEGLIANZA | LUOGHI DI LAVORO

Art.4 c.3 L. 300/1970 «Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro, **compresi i fini disciplinari**, a condizione che:



Sia data al lavoratore **adeguata informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli...

...nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196» (TU Privacy) | in armonizzazione al GDPR | vedi anche 88 GDPR.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

259

VIDEOSORVEGLIANZA | DPIA

Al Punto 5 dell'**elenco delle tipologie di trattamenti** soggetti al requisito di valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 **pubblicato dall'Autorità di controllo** – Provv. 467 del 11 ottobre 2018 [9058979] si annoverano:



«Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai **sistemi di videosorveglianza** e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri n. 3, 7 e 8)».

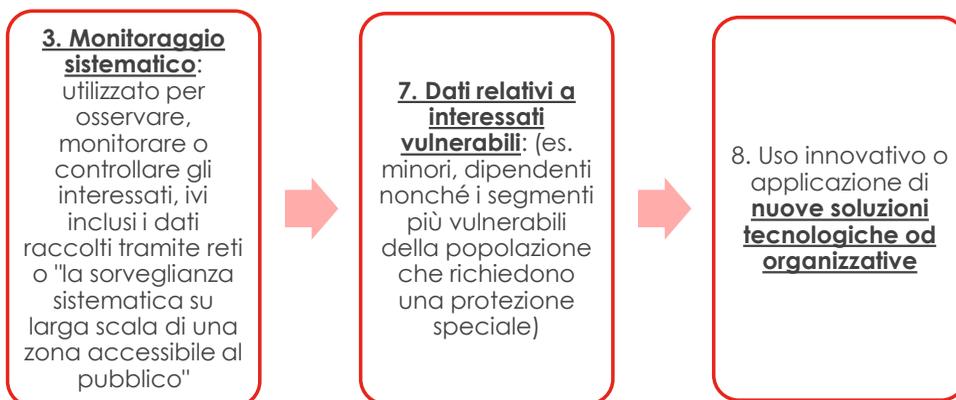
Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

260

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

VIDEOSORVEGLIANZA | DPIA

Criteria imposti dal WP 29
(«linee guida per lo svolgimento di un DPIA» - 4 aprile 2017):



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

261

VIDEOSORVEGLIANZA | DPIA

Nel caso in cui la DPIA indichi un rischio elevato, il titolare dovrà provvedere ad una **consultazione preventiva** dell'Autorità Garante Privacy (Art. 36 GDPR).



<https://www.garanteprivacy.it/>



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

262

BIOMETRIA | PROVVEDIMENTO N. 513/2014

Con il Provvedimento Generale prescrittivo in tema di biometria n. **513/2014**, il Garante Italiano ha adottato le **Linee Guida in materia di riconoscimento biometrico e firma grafometrica (Allegato A)** che individuano, per i vari tipi di trattamento che possono essere effettuati:



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

263

POSIZIONE EUROPEA | RICONOSCIMENTO FACCIALE

NEWS UE → volontà di porre un *blocco* per tre o cinque anni, all'*utilizzo del riconoscimento facciale* in luoghi pubblici per esigenze di sorveglianza



Diversamente negli U.S.A. → diversi agenti della Polizia stanno utilizzando software di riconoscimento facciale che promette di riconoscere in tempo reale il volto delle persone comparandolo, con un database di oltre tre miliardi di foto costituito tramite il web (incominciando da Facebook).

E la compliance Privacy?

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

264

BIOMETRIA | PROVVEDIMENTO N. 513/2014

Cosa sono i dati biometrici?

Art. 4 - Definizione

«dati personali ottenuti da un trattamento tecnico specifico relativi alle **caratteristiche fisiche, fisiologiche o comportamentali** di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

265

BIOMETRIA | PROVVEDIMENTO N. 513/2014



Coerentemente con i **pareri del WP 29** possiamo considerare **quindi** dati biometrici: i campioni, modelli, riferimenti, tratti biometrici e ogni altro dato ricavato con **procedimento informatico** da caratteristiche biometriche e che possa essere ricondotto ad un **interessato, individuato o individuabile**

↓
dato personale

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

266

BIOMETRIA | PRINCIPI GENERALI

Il **trattamento dei dati biometrici** si deve svolgere in conformità alle disposizioni del Codice e del GDPR, nel rispetto dei principi generali:

- Liceità
- Necessità
- Finalità
- Proporzionalità



BIOMETRIA E DPIA

Il trattamento di dati biometrici rientra nell'elenco delle tipologie di **trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati | DPIA** ai sensi dell'art. 35 GDPR.

In particolare, al punto n. 11 della lista pubblicata in data 11 novembre 2018 dal Garante italiano - composta da **12 macro-tipologie di trattamento** – si annoverano:



«Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento».

BIOMETRIA | PROVVEDIMENTO N. 513/2014

Per riassumere...

In caso di trattamento di dati biometrici, ferma restando la necessità di rispettare i principi di liceità, finalità, necessità, proporzionalità e fornire idonea **informativa** occorre valutare la necessità di:

- Predisposizione **Valutazione d'impatto sulla protezione dei dati | DPIA** ;
- **Verificare le misure di garanzia richieste dal Garante ai sensi dell'art.2 septies;**
- Consultazione preventiva – se necessaria;

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

269

DOMANDE



Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

270

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE

IL DOCENTE

AVV. ELISA MARINI



Avvocato. Formatrice, esperta nella consulenza in materia di Privacy e contrattualistica. Ha conseguito la certificazione UNI 11697 come Data Protection Officer ed è Valutatore Interno ISO 27001 qualificato da Bureau Veritas Italia SpA.

Copyright © 2020 Labor Project. Tutti i diritti sono riservati. È vietata la riproduzione.

271



GRAZIE PER L'ATTENZIONE

www.laborproject.it

272

IL MANUALE È AD USO ESCLUSIVO DEI CORSISTI: NE È VIETATA LA RIPRODUZIONE