Tutela della privacy

"Regolamento Europeo"
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679

Davide Candia

Maurizio Provenzano

Francesco La Franca

“Regolamento Europeo”
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679

pubblicato in GUUE il 04/05/16

ART. 1 GDPR
Oggetto e finalità

- Il presente regolamento stabilisce norme relative alla protezione **delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

- 2.Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

- 3.La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Art.2 Costituzione

- “la Repubblica riconosce e garantisce i diritti inviolabili dell’uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l’adempimento dei doveri inderogabili di solidarietà politica, economica e sociale”

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA

- articolo 8, paragrafo 1, e l'articolo 16, paragrafo 1, del trattato stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

a) Trattamento

- Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

a) Trattamento

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- la organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera;
- la elaborazione, ovvero le operazioni che attribuiscono significatività ai dati, in relazione allo scopo per il quale essi sono stati raccolti;

b) Dato personale

- Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
- Nominativo, indirizzo o altri elementi di identificazione personale
- nome, cognome, età, sesso, luogo e data di nascita
- indirizzo privato, indirizzo di lavoro, numero di telefono, numero di telefax o di posta elettronica
- posizione rispetto agli obblighi militari
- dati fisici (altezza, peso, ecc.)
- dati idonei a rivelare l'origine nazionale

b) Dato personale

- Codice fiscale ed altri numeri di identificazione personale
- carte sanitarie
- numero carta di identità, passaporto, patente di guida, numero di posizione previdenziale o assistenziale
- targa automobilistica
- Istruzione e cultura
- curriculum di studi e accademico
- pubblicazioni: articoli, monografie
- Lavoro
- occupazione attuale e precedente
- informazioni sul reclutamento, sul tirocinio o sulla formazione professionale
- informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione
- curriculum vitae o lavorativo, competenze professionali
- dati relativi alle pregresse esperienze professionali

d) Dati sensibili

- Idonei a rivelare le origini razziali o etniche
- dati idonei a rivelare l'appartenenza ad un gruppo linguistico
- Idonei a rivelare le convinzioni religiose; adesioni ad organizzazioni a carattere religioso (registri dello stato civile)
- Idonei a rivelare le convinzioni filosofiche o di altro genere e le adesioni ad organizzazioni a carattere filosofico
- Idonei a rivelare le opinioni politiche (liste elettorali)
- Idonei a rivelare la adesione a partiti od organizzazioni a carattere politico
- Idonei a rivelare la adesione a sindacati o organizzazioni a carattere sindacale
- Idonei a rivelare lo stato di salute
- dati idonei a rivelare l'appartenenza a categorie protette
- dati idonei a rivelare l'identità del donatore
- dati idonei a rivelare l'identità del ricevente

d) Dati sensibili

- dati idonei a rivelare lo stato di disabilità
- dati idonei a rivelare sieropositività
- dati idonei a rivelare malattie infettive e diffusive
- dati idonei a rivelare malattie mentali
- dati relativi a indagini epidemiologiche
- dati relativi a prescrizioni farmaceutiche e cliniche
- dati relativi ad esiti diagnostici e programmi terapeutici
- dati relativi all'utilizzo di particolari ausili protesici
- dati relativi alla prenotazione di esami clinici e visite specialistiche
- dati idonei a rivelare AIDS conclamato
- dati inerenti a caratteristiche o idoneità psichiche
- Idonei a rivelare la vita sessuale (registri dello stato civile)
- dati idonei a rivelare lo stato di gravidanza
- dati idonei a rivelare il cambiamento di sesso

d) Dati genetici

- Dati idonei a rilevare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali
- Dati idonei a rilevare la gravità o il decorso del quadro clinico delle patologie genetiche
- Dati idonei a identificare malattie ereditarie
- Dati relativi alle malformazioni congenite la cui causa non è nota
- Dati idonei ad accertare maternità o paternità
- Dati relativi a indagini epidemiologiche
- Dati relativi a indagini sulla popolazione
- Dati relativi a trapianti di tessuti od organi o all'impiego di cellule staminali
- Dati relativi alla procreazione
- Dati tratti da studi di relazione tra patrimonio genetico e fattori di rischio

d) Dati biometrici

- Caratteristiche della voce
- Geometria della mano
- Impronte digitali
- Informazioni di tipo comportamentale (andatura, movimento delle labbra, digitazione su tastiera...)
- Riconoscimento dell'iride o retina
- Rilevazione facciale attraverso uno o più elementi

e) Dati giudiziari

- I dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma1, lettera da a) a o) e da r) a u), del D.P.R. 14 novembre 2002 n. 313 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del c.p.p

“Regolamento Europeo”
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679

pubblicato in GUUE il 04/05/16

COSA E' CAMBIATO ?

DIRITTO ALL'OBLIO

COSA E' CAMBIATO ?

PORTABILITA' DEI DATI

COSA E' CAMBIATO ?

ABOLIZIONE DELLA NOTIFICAZIONE

COSA E' CAMBIATO ?

DATA BREACH

COSA E' CAMBIATO ?

SANZIONI PARI AL 2-4% DEL FATTURATO

Ambiti di Applicazione – Art. 3

Il Regolamento si applica a:

Imprese con almeno uno stabilimento nell'Unione

Indipendentemente dal fatto che il trattamento sia effettuato nell'UE

Imprese che non hanno uno stabilimento nell'UE, nei seguenti casi:

Offerta di beni o servizi (anche gratuiti) agli Interessati nel territorio dell'UE

Monitoraggio del comportamento degli Interessati all'interno dell'Unione

Imprese che non hanno uno stabilimento nell'UE, ma:

Con stabilimento in un luogo soggetto al diritto di uno Stato Membro

Il Regolamento trova applicazione anche nei confronti di Big Data e c.d. colossi del web (Facebook, Google, etc.)

Art. 27: Nei casi di soggetti che non hanno uno stabilimento nell'UE, il Titolare o il Responsabile designa per iscritto un Rappresentante nell'Unione. Tale obbligo non si applica ai trattamenti occasionali e alle autorità o organismi pubblici.

Il Rappresentante non è solamente un interlocutore, ma è anche soggetto ad eventuali atti di esecuzione, fatte salve le azioni legali nei confronti del Titolare o del Responsabile del trattamento.

“Nuove Definizioni e Categorie di Dati”

Soggetti Coinvolti

Codice Privacy:	Regolamento Europeo:
	
Titolare del Trattamento	Data Controller o Titolare del Trattamento
	
Responsabile Esterno del Trattamento Amministratore di Sistema	Joint Controller o Contitolare del Trattamento
	
Responsabile ed Incaricato del Trattamento	Data Processor o Responsabile del Trattamento
	
Responsabile della Sicurezza dei Dati Personali	Data Protection Officer

Titolare o Responsabile? – Capo IV

Il testo originale del Regolamento Europeo prevedeva solo la figura di Responsabile del Trattamento e dell'Incaricato.

Il 13 aprile 2016 il Garante della Privacy ha annunciato che la traduzione italiana del Regolamento avrebbe mantenuto la struttura gerarchica già presente nel Codice Privacy, andando ad introdurre nuovamente la figurare del Titolare del Trattamento.

I termini "Titolare del trattamento" e "Responsabile del trattamento", già presenti nel Codice privacy italiano, compariranno anche nei testi italiani del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i settori di prevenzione, contrasto e repressione dei crimini, entrambi in invia di approvazione definitiva a Bruxelles.

Si tratta di un adattamento terminologico caldeggiato dal Garante per la protezione dei dati personali preoccupato di non veder sottoposti gli operatori del nostro Paese ad un inutile sforzo adattativo e interpretativo. L'iniziativa del Garante ha trovato anche il sostegno dei giuristi-linguisti di lingua italiana presso il Consiglio e il Parlamento Ue.

Le precedenti versioni italiane del Regolamento, infatti, riportavano i termini "responsabile del trattamento" (data controller) e "incaricato del trattamento" (data processor). Tuttavia, trattandosi, di fatto, di figure identiche quanto a caratteristiche soggettive a quelle che nel Codice privacy italiano sono indicate rispettivamente come "titolare" e "responsabile", l'Autorità italiana ha chiesto ed ottenuto che i nuovi testi mantenessero tali diciture in modo da evitare a imprese, enti, professionisti e cittadini ogni possibile problema di interpretazione giuridica ed eventuali costi, anche materiali, connessi al cambiamento terminologico.

Il TITOLARE DEL TRATTAMENTO

- Il Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza.

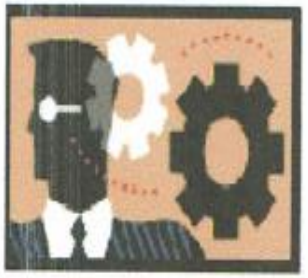
- E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che:

- assicurino e garantiscano che vengano adottate le misure di sicurezza previste dal GDPR e del Codice in materia di trattamento dei dati personali;

- adottino delle misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il RESPONSABILE (2/3)

"Interno"



- *Coadiuva il Titolare negli obblighi privacy*
- *Nomina opzionale*
- *"Obbligata" se organizzazione complessa*
- *Deve presentare adeguate garanzie di competenza*
- *Ha assegnato compiti scritti e riceve istruzioni*
- *Puo' designare gli incaricati*

CHI PUO' ESSERE IN AZIENDA?

PERSONA DI ALTO PROFILO / COMPETENZA

(es. Dir. Legale, Personale, Vendite, Organizzazione, Compliance Manager...)

Il RESPONSABILE (3/3)

"Esterno"

- Soggetto che tratta dati per conto del Titolare
- New Ruolo "obbligatorio" in caso di esternalizzazione di attività (es: predisposizione cedolini, gestione sistema informativo, call center, agenti...)
- Puo' essere persona fisica o giuridica
- Deve presentare adeguate garanzie di rispetto del Regolamento
- New I trattamenti esternalizzati devono essere disciplinati da un contratto (o atto giuridico) scritto, sottoscritto per accettazione
- New Il contratto deve prevedere una serie di vincoli prestabiliti (art28)

CHI E' ALL' ESTERNO DELL' AZIENDA

CIASCUN OUTSOURCER

E gli Incaricati?

Il testo del regolamento fa riferimento in più punti a *persone autorizzate al trattamento*, senza però fornire una precisa definizione o un ruolo (Art. 30 Codice Privacy: Incaricati / Data Handler).

La figura dell'Incaricato è rilevante soprattutto in ottica di Accountability, poiché potrebbe essere utile nel dimostrare l'adozione di tutte le misure tecniche ed organizzative adeguate a garantire un trattamento conforme dei dati, e nell'individuare i centri di responsabilità privacy.

Etichettare i ruoli è fondamentale poiché favorisce la rintracciabilità dei Soggetti coinvolti nel trattamento dei dati, soprattutto da parte dell'Interessato.

Il GDPR non mette in discussione l'Incaricato del Trattamento (ex art. 30 196/03). Tale articolo non è in conflitto, ma compatibile con GDPR, pertanto potrebbe rimanere in vigore. Il GDPR abroga la Direttiva 95/46, non Codice il Privacy.

Nella 27001 e nella 231 la sicurezza informatica e la correttezza del trattamento dipendono quasi esclusivamente dalla persona autorizzata al trattamento dei dati. Nell'ottica della 231, l'adeguatezza del Modello Organizzativo Privacy è fondamentale anche da un punto di vista penale, al fine di determinare i soggetti responsabili penalmente.

INCARICATI DEL TRATTAMENTO

- Tutti gli operatori che trattano dati personali devono almeno essere designati, ancora con atto scritto, quali “incaricati del trattamento”. Ogni incaricato deve attenersi alle istruzioni ricevute dal responsabile. La nomina degli Incaricati del trattamento deve essere controfirmata dall’interessato per presa visione e copia della stessa deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.

- Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

INCARICATI DEL TRATTAMENTO

- La nomina degli Incaricati è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.
- Nell'assolvimento del loro compito gli Incaricati del Trattamento dovranno osservare scrupolosamente le seguenti istruzioni:

ISTRUZIONI PER GLI INCARICATI

- Al primo accesso alle banche dati, delle quali effettueranno il trattamento, ogni incaricato provvederà a modificare la password assegnatagli e a modificarla ogni sei mesi. Nel caso venissero trattati dati sensibili o giudiziari, la password andrà modificata ogni tre mesi. Sarà cura di ogni incaricato garantire la segretezza delle proprie credenziali di autenticazione

Joint Controller – Art. 26

Si tratta del così detto Titolare Congiunto, o meglio ancora del Contitolare del Trattamento dei Dati: nello specifico, per un medesimo trattamento di dati personali, potranno sussistere due responsabili del trattamento.

Titolare del Trattamento

Joint Controller

Se più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono Contitolari del trattamento e determinano le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal Regolamento.

I Contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi.

Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato, che può esercitare i propri diritti nei confronti di ciascun soggetto. Ma l'Autorità Garante quale soggetto andrebbe a colpire in caso di illecito?

Categorie di Dati Attuali

Dati Comuni

- Anagrafici
- Indirizzi Postali/Telematici
- Codici Indentificativi

Dati Giudiziari

- Iscrizioni casellario giudiziario in materia penale, condanna, abitualità nel reato, ecc

Dati Quasi Sensibili

- Presentano rischi per libertà/dignità
- Accorgimenti dettati dal Garante: «Prior Checking»

Dati Sensibili

- Origine raziale / etnica
- Convinzioni religiose, filosofiche, politiche
- Stato di Salute / Vita sessuale

Attuale Definizione di Dati Sensibili

Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti e sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Medico Sanitari

Vita Sessuale

I Dati Sensibili diventano Particolari – Art. 9

Dati personali che rivelino razza, origine etnica, opinioni politiche, religione o le convinzioni personali, appartenenza sindacale, dati relativi alla salute, alla vita e orientamento sessuale, come anche dati genetici e biometrici, ~~o dati relativi a condanne penali o a connesse misure di sicurezza~~.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Relativi alla Salute

Vita Sessuale

Dati Biometrici

Dati Genetici

~~Condanne Penali e Reati~~

Diventa lecito trattarli se il trattamento riguarda dati resi manifestamente pubblici dall'interessato.

Dati Relativi alla Salute – Art. 9

Per il trattamento di dati relativi alla salute del soggetto Interessato anche per prestazioni sanitarie, di diagnosi e cura, non servirà più il consenso dell'Interessato, se tali dati vengono trattati da personale medico-sanitario, in quanto gli stessi soggetti sono tenuti al rispetto del segreto professionale.

Dati Relativi alla Salute anche per Prestazioni di Diagnosi e Cura

Trattati da Personale tenuto al Segreto Professionale

Non Necessario il Consenso

Dati Relativi a Condanne Penali – Art. 10

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, può avvenire soltanto sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati.

Condanne Penali e Reati

Sotto il Controllo dei Pubblici Poteri

Autorizzato dal diritto dell'Unione o Stati membri

Adeguate Garanzie per Diritti e Libertà degli interessati

Un registro completo delle condanne penali può essere tenuto soltanto sotto il controllo dei pubblici poteri.

“Principi introdotti dal Regolamento e modifiche apportate”

Principio di Accountability - Art. 24

~~Il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al presente regolamento.~~

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento.

Campo di Applicazione, Contesto, Finalità, Rischi e Gravità per i Diritti

Misure Tecniche e Organizzative Adeguate

Onere della Prova: Dimostrare che il Trattamento è Conforme

New

ACCOUNTABILITY

Responsabilizzazione e obbligo generale di Prova degli adempimenti –art 24

- **CHI E' OBBLIGATO**
  - *IL TITOLARE*
- **COSA DEVE FARE**
  - ***OPERARE***
    - ✓ *Mettere in atto misure Tecniche e Organizzative adeguate*
    - ✓ *Anche mediante pubblicazione e attuazione di politiche adeguate*
  - ***DARE DIMOSTRAZIONE***
    - ✓ *Essere in grado di dimostrare che i trattamenti avvengono in conformità al Regolamento*
  - ***AGGIORNARE***
    - ✓ *Verificare periodicamente le misure e aggiornarle*

NOTA: *Il rispetto degli obblighi può essere dimostrato attraverso l'adesione a codici di condotta o al meccanismo di certificazione (art 40,42)*

Informativa Chiara e Semplice - Art. 13

Il Titolare del trattamento fornisce all'interessato tutte le informazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare le informazioni destinate specificamente ai minori.

Identità del Titolare (e DPO)

Finalità del Trattamento

Base Giuridica del Trattamento

Legittimi Interessi Perseguiti

Destinatari dei dati personali

Trasferimento dei Dati

Periodo di Conservazione dei Dati

Diritto di Accesso ai Dati

Revoca del Consenso

Diritto di Proporre Reclamo

Obbligatorietà comunicazione Dati

Processi Automatizzati (Profilazione)

Informativa - Art. 14

In caso di dati non raccolti presso l'Interessato è inoltre necessario fornire queste ulteriori informazioni:

Categorie dei Dati

Fonte da cui hanno origine i Dati

Eventuale provenienza da fonti accessibili al pubblico

Il Titolare deve fornire l'informativa al massimo entro un mese dall'ottenimento dei dati o al momento della prima comunicazione con l'Interessato o divulgazione degli stessi.

In caso di trattamento dei dati per ulteriori finalità occorre fornire una nuova informativa all'Interessato.

Casi di esclusione:

L'Interessato dispone già di tali informazioni

La comunicazione è impossibile o implica risorse sproporzionate

Trattamento previsto dal diritto degli Stati Membri e UE

Trattamento soggetto a Segreto Professionale

Consenso Inequivocabile - Art. 4

Consenso dell'Interessato: qualsiasi manifestazione di volontà libera, specifica, informata ~~ed esplicita~~ con la quale l'Interessato accetta, mediante dichiarazione o **azione positiva inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento.

Rimosso il termine "Consenso Esplicito" dal testo

Passaggio al "Consenso Inequivocabile" ovvero anche per "Fatti Concludenti"

Non configura consenso il consenso tacito o passivo o la preselezione di caselle

Se il consenso è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso.

IL CONSENSO (1/4)

Condizione di LICEITA'

COS'E'

- *E' la condizione necessaria per poter trattare i dati in modo lecito, in assenza di una delle altre condizioni previste dalla legge (es. esecuzione contratto, obbligo di legge...)*
- *Deve essere richiesto in chiusura dell'Informativa*
- *Risposta dell'interessato all' Informativa*

SCOPO

- *Autorizzare o negare l'uso dei dati*

CONDIZIONI DI VALIDITA'

- ***INFORMATO** invalido se non preceduto da informativa*
- ***SPECIFICO,** richiesto in modo chiaro e distinguibile dal resto*
- New ***LIBERO** svincolato da costrizioni . es. l'esecuzione del contratto non deve essere subordinata al rilascio del Consenso per l' invio di pubblicità*
- New ***CONSAPEVOLE E INEQUIVOCABILE,** basato su dichiarazione o azione positiva- No caselle pre-barrate*

IL CONSENSO (2/4)

- **LA PLURALITA' DEI CONSENSI**
  - ***Diritto di esprimere Consenso per una o più finalità***
  - ***Esempi di finalità aggiuntive:***
    - ✓ *Profilazione,*
    - ✓ *Invio di pubblicità non richiesta,*
    - ✓ *Comunicazione a terzi diversi da Responsabile e Incaricati ,*
    - ✓ *Trasferimento dati extra UE*
    - ✓ *.....*
- **GRANULARITA'**
  - ***Richiesta Consenso distinto e separato per ciascuna finalità***

IL CONSENSO (3/4)

- **QUANDO DEVE ESSERE DISPONIBILE**
  - *Prima del trattamento*

- **IN CHE FORMA**
  - *In forma scritta . Se orale, va documentata*

- **DIMOSTRABILITA'**
  - *Il Titolare deve essere in grado di darne dimostrazione*
  - *Opportuno prevedere una modulistica, chiara e semplice*

New

- **DIRITTO DI REVOCA**
  - *Revocabile in qualsiasi momento*
  - *Il Titolare deve informare di ciò l'Interessato*

New

IL CONSENSO (4/4)

- **QUANDO E' NECESSARIO**
  - *Se non ricorre un altro caso di liceità previsto dal Regolamento*

- **QUANDO <u>NON</u> E' NECESSARIO: *CASI DI LICEITA' -art 6***
  - *Per i trattamenti necessari ad eseguire un contratto o per eseguire misure precontrattuali su richiesta dell'interessato*
  - *Per adempiere ad un obbligo legale*
  - *Per la salvaguardia degli interessi vitali dell'interessato o di altra persona*
  - *Per un compito di interesse pubblico*
  - New *Per il perseguimento del legittimo interesse del Titolare (salvo che non prevalgano i diritti fondamentali dell'interessato)*

New *in tali casi non va richiesto*

IL CONSENSO
PER IL MARKETING

- **ATTIVITA' DI MARKETING NON RICHIESTO**
  - *Le Regole sono contenute nella Direttiva UE sulle Comunicazioni elettroniche , recepite dal Codice Privacy, art 130 che rimane in vigore.*

- **COSA SI INTENDE PER MKTG NON RICHIESTO**
  - *Attività promozionale su iniziativa del Titolare*
  - *Eesempio : invio materiale pubblicitario e simili tramite e-mail , fax , SMS, Marketing telefonico e postale*

- **CONDIZIONE DI LICEITA'**
  - *Consenso espresso in varie forme, Diritto di Opposizione*

- **APPLICABILITA'**
  - *Non solo persone fisiche ma anche persone giuridiche*

IL DIRITTO DI CONTROLLO SUI PROPRI DATI

- **SCOPO**
  - *Dominio sui dati e Verifica di correttezza (art.15-22)*

- **COSA COMPRENDE**
  - *DIRITTO DI ACCESSO*
  - *DIRITTO DI RETTIFICA*
  - New *DIRITTO ALL' OBLIO*
  - New *DIRITTO DI LIMITAZIONE DEL TRATTAMENTO*
  - New *DIRITTO ALLA PORTABILITA' DEI DATI.*

Riscontro al Diritto d'Accesso - Art.12

- Mentre il Codice Privacy prevede 15 giorni di tempo (più ulteriori 15 in caso di complessità di reperimento di informazioni), il Regolamento Europeo aumenta il termine a 30 giorni, più ulteriori 30 giorni (2 mesi) in caso di complessità se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento e del numero di richieste.

In caso di dubbi circa l'identità della persona fisica, il Titolare del trattamento può richiedere ulteriori informazioni.

Le informazioni possono essere fornite in combinazione con icone standardizzate. L'Interessato è informato dei motivi del ritardo entro 30 giorni dal ricevimento della richiesta

Registro delle Opposizioni
Fondazione Ugo Bordoni
Robinson List

- Il Ministero dello sviluppo economico istituisce, ai sensi dell'articolo 130, comma 3-bis, del Codice, e sulla base delle disposizioni di cui all'articolo 4, il registro pubblico delle opposizioni

- La Fondazione Ugo Bordoni è un'Istituzione di Alta Cultura e Ricerca, sottoposta alla vigilanza del Ministero dello Sviluppo Economico. www.fub.it/
- http://www.registrodelleopposizioni.it/.

Minori Più Protetti – Art. 8

Il trattamento di dati personali di minori di età inferiore di minori al di sotto dei 16 anni - o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni - è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore.

Il Titolare del Trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia espresso o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

VIETATO ai MINORI

Uniformazione del concetto di «minore di anni 18»

Il trattamento dei Dati di minori ~~di anni 13~~ verrà subordinato al consenso da parte di un genitore

Modificato in: minori di 16 anni o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni

Profilazione – Art. 22 – Testo Definitivo

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 allo stesso modo significativamente sulla sua persona.

Tale articolo non si applica nel caso in cui la decisione:

Sia necessaria per la conclusione o l'esecuzione di un contratto.*

Sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il Titolare del trattamento.

Si basi sul consenso esplicito dell'Interessato.*

* In questi casi il Titolare del Trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano da parte del Responsabile del Trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni basate sul trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell'interessato non possono basarsi unicamente sulle categorie particolari di dati personali.

Principio di Minimizzazione – Art. 5

Testo Commissione LIBE: Il principio di minimizzazione dei dati prevede una raccolta, memorizzazione ed elaborazione di dati personali, solo se adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Raccolta

Conservazione

Elaborazione

Il testo della Commissione LIBE faceva riferimento a «Dati Limitati al Minimo Necessario»

Il testo del Consiglio Europeo eliminava tale principio, limitandolo a un «Dati Non Eccessivi»

Nel testo definitivo vengono introdotti «Dati Limitati a Quanto Necessario»

Diritto all'Oblio – Cancellazione dei Dati
Art. 17

L'Interessato ha il diritto di ottenere la cancellazione dei propri dati ~~e la rinuncia ad una ulteriore diffusione degli stessi~~.

Il Titolare del trattamento che rende pubbliche delle informazioni è tenuto a prendere tutte le misure ragionevoli, anche tecniche, per informare ~~i soggetti terzi, che a loro volta trattano tali dati,~~ i Titolari di un'eventuale richiesta di cancellazione da parte di un soggetto interessato, al fine di provvedere anch'essi all'eliminazione di qualsiasi link, copia o riproduzione dei dati personali.

~~Il Responsabile del trattamento è responsabile anche della pubblicazione dei dati effettuata da soggetti terzi, qualora siano stati autorizzati dallo stesso.~~

Corte di Giustizia Europea nella celebre sentenza "Google Spain/Inc. v. Agencia Española de Protección de Datos (AEPD)/Mario Costeja González" del 13 maggio 2014

New

IL DIRITTO ALL'OBLIO

- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *CANCELLARE I DATI*
    - ✓ *se è esaurita la finalità del trattamento*
    - ✓ *se è stato revocato il Consenso*
    - ✓ *se è stata fatta Opposizione al trattamento*
    - ✓ *se trattati in violazione di legge.*

- **RAFFORZAMENTO PER INTERNET**
  - *OBBLIGO DEL TITOLARE "EDITORE" DEI DATI*
    - ✓ *Informare altri Titolari di cancellare i link*

Diritto all'Oblio – Casi di Esclusione

Il diritto alla cancellazione non si applica qualora il trattamento dei dati sia necessario per:

Libertà di Espressione e di Informazione

Adempimento Obblighi Legali

Interesse Pubblico in ambito Sanitario

Interesse Storico, Scientifico, Statistico

Difesa di un Diritto in Sede Giudiziaria

L'Interessato ha il diritto di ottenere la limitazione del trattamento dei dati nei seguenti casi:

Contestazione dell'esattezza dei Dati

Trattamento Illecito dei Dati (se richiesto)

Difesa di un Diritto in Sede Giudiziaria

In Caso di Opposizione al Trattamento

Diritto all'Oblio – Portabilità dei Dati

Art. 20

Diritto per il soggetto Interessato di ricevere dal Titolare del trattamento copia dei propri dati personali, in formato elettronico strutturato, di uso comune e leggibile a macchina, al fine di consentirgli ~~un ulteriore agevole utilizzo~~ la trasmissione ad un altro Responsabile del trattamento.

Il testo definitivo introduce per l'Interessato il diritto di ottenere la trasmissione diretta dei dati da un Titolare del trattamento ad un altro, se tecnicamente fattibile.

Si tratta di un diritto che non è applicabile ai Titolari del trattamento (società) rispetto all'allocazione di dati su sistemi di soggetti terzi (cloud). Tale diritto è riconosciuto, infatti, solamente ai soggetti Interessati per la tutela dei propri dati personali.

New

IL DIRITTO ALLA PORTABILITA' DEI DATI

- **OBIETTIVO**
  - *SEMPLIFICARE CAMBIO DI FORNITORE*
- **QUANDO PUO' ESERCITARE IL DIRITTO**
  - *In caso di trattamento necessario per eseguire contratto*
  - *In caso di dati basati su Consenso*
- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *IN CASO DI TRATTAMENTO AUTOMATIZZATO*
    - ✓ *Ricevere i dati in formato chiaro e leggibile*
    - ✓ *Ottenere il trasferimento automatico ad altro Fornitore, ove fattibile.*

New

IL DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *LIMITARE IL TRATTAMENTO*
    - ✓ *In caso di dati inesatti, fino alla rettifica*
    - ✓ *In caso di contestazione, fino a chiarimento*
    - ✓ *Su richiesta, in alternativa alla cancellazione*

- **OBBLIGO DEL TITOLARE: DEFINIRE LA MODALITA'**
  - ✓ *Trasferire i dati ad altro sistema*
  - ✓ *Rendere i dati inaccessibili*
  - ✓ *Rimuovere temporaneamente i dati*
  - ✓ *Congelare i dati*
  - ✓ *In ogni caso, identificarli nel sistema*

Aziende Extra UE – Capo V

Il Regolamento Europeo impone che si applichi la normativa UE qualora un "Azienda Extra-CEE" rivolga servizi o prodotti al mercato UE.

Ciò significa che un'impresa non europea che opera nell'ambito dell'unione sarà tenuta a rispettare e a recepire integralmente i nuovi obblighi introdotti dalla riforma e a garantire lo stesso livello di tutela e riservatezza delle informazioni di una qualunque azienda europea.

Trasferimento Extra-CEE dei Dati

Qualunque organizzazione con sede al di fuori dell'Unione Europea che tratti dati derivanti dalle filiali europee sarà tenuto a farlo nel rispetto totale del nuovo regolamento, applicando gli stessi principi e recependo gli stessi obblighi previsti per trattamenti effettuati nella stessa UE.

Trasferimento Extra-CEE

Rispettando il Regolamento Europeo

Via libera ai trasferimenti di dati verso Paesi terzi, anche se sprovvisti di una legge sulla protezione dei dati, attraverso la predisposizione di codici di condotta e accordi, come ad esempio le BCR (Binding Corporate Rules), Safe Harbor (ad esclusione degli USA) e UE-USA Privacy Shield.

“Obblighi del Titolare del Trattamento”

Data Protection Impact Assessment – Art. 35

Quando il trattamento, per la sua natura, campo di applicazione, contesto o finalità, presenta rischi ~~specifici~~ elevati per i diritti e le libertà ~~degli interessati~~ di persone fisiche, il Titolare del Trattamento è tenuto ad effettuare una valutazione dell'impatto del trattamento previsto sulla protezione dei dati personali.

DATA	N° RIF	OGGETTI SOTTOPOSTI A CONTROLLO	CONFORMITÀ	NOTE SULLA CONFORMITÀ	IMPATTO DEL RISCHIO	INDICE DEL RIS			SANZIONE
15/09/14	01.01	**Individuazione del Titolare del Trattamento dei dati**	**Conforme**	Nei casi in cui tutti i poteri e le responsabilità derivanti dall'esercizio di un'attività non siano in capo ad un unico vertice (es. Amministratore unico) si rende necessario individuare un soggetto che rivesta la figura del Titolare del Trattamento dei dati con poteri di delega e di firma.	Rischio di mancata Identificazione del Titolare del Trattamento di dati che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.	1	1	1	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**
15/09/14	01.02	**Nomina dei Responsabili e degli Incaricati al Trattamento dei dati**	**Parzialmente conforme**	Sono stati designati gli Incaricati al Trattamento dei dati, ma non sono stati nominati i Responsabili del Trattamento. Nomina Responsabile della Sicurezza dei dati e del Trattamento:ASSENTI. Le lettere di incarico sono state redatte e risultano essere conformi.	Rischio di mancata Identificazione del Personale interno ad esterno preposto allo svolgimento di compiti specifici e relativi Trattamenti di dati.	2	3	6	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**
15/09/14	01.04	**Identificazione dei Responsabili al Trattamento in Out-Sourcing**	**Non Conforme**	Non sono stati identificati i Responsabili al Trattamento dei dati in Out--Sourcing con relativa nomina.	Rischio di mancata Identificazione dei Responsabili in Out-Sourcing preposti a Specifici Trattamenti dei dati.	3	3	9	Omessa Adozione di Misura Minima di Sicurezza **Arresto sino a due anni, Sanzione Amministrativa da € 10.000 a 120.000**

Data Protection Impact Assessment – Art. 35

La valutazione è richiesta in particolare nei seguenti casi:

Profilazione o valutazione di aspetti personali che influiscono su decisioni con effetti giuridici o incidono su persone fisiche

Trattamento su larga scala di Dati Particolari o relativi a condanne penali

Sorveglianza sistematica di zona accessibile al pubblico su larga scala

L'Autorità di controllo redige e rende pubblico l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Data Protection Impact Assessment-Art. 35

La valutazione deve contenere almeno:

Descrizione sistematica dei trattamenti e delle finalità

Valutazione su necessità e proporzionalità dei trattamenti

Valutazione di rischi per i diritti e le libertà degli interessati

Misure previste per affrontare i rischi

Misure di Sicurezza Adeguate - Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati

Divulgazione non autorizzata dei Dati

Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Protezione fisica delle aree e dei locali

- Le misure antintrusione (intese come perimetrazione, compartimentazione dei locali e la video-sorveglianza di edifici e locali)

- Le misure antincendio (da considerare obbligatorie ai sensi del D.Lgs 81/08 -D.lgs 106/09)

Protezione fisica delle aree e dei locali

- UPS Gruppi di continuità per PC
- UPS per le linee telefoniche
- Protezione degli archivi cartacei e conservazione sicura dei supporti di memorizzazione (disco rigido rimovibile, cd/dvd, pen drive)
- Regole per il controllo degli accessi fisici ai locali dell'azienda

LA SICUREZZA DEL TRATTAMENTO- art 32

- **SCOPO**
  - Garantire la sicurezza dei dati e prevenire rischi di danni agli Interessati

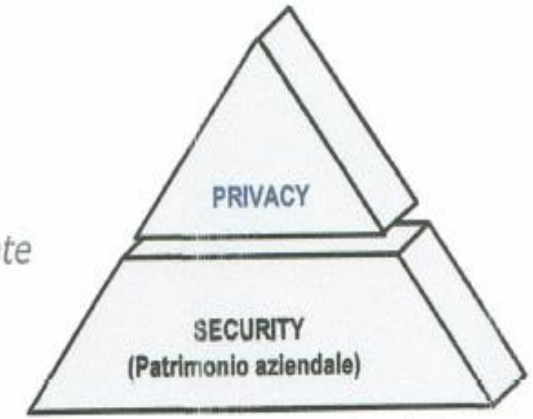
- **DESTINATARI DELLA NORMA**
  - Titolare
  - Responsabile
  - Incaricato

- **RESPONSABILITA'**
  - ***TITOLARE E RESPONSABILE***
    - ✓ Individuare e adottare le Misure di Sicurezza
    - ✓ Fornire agli Incaricati istruzioni/formazione al riguardo
    - ✓ Vigilare su efficacia
  - ***INCARICATI***
    - ✓ Trattare i dati secondo le istruzioni ricevute
    - ✓ Comportamento consapevole dei rischi

La Sicurezza Del Trattamento
COSA DEVE ESSERE FATTO

- **RISK ASSESSMENT**
  - *Relativo agli strumenti*
  - *Relativo al contesto*
  - *Relativo al comportamento*

- **MISURE DI CONTRASTO DEI RISCHI**
  - *Adottare misure di sicurezza che comprendano*
    - *Garanzia di*
      - ✓ *disponibilità dei dati*
      - ✓ *integrità dei dati*
      - ✓ *riservatezza dei dati*
      - New ✓ *resilienza dei sistemi e dei servizi*
    - *Uso di pseudonomi e cifratura dei dati*
    - *Ripristino tempestivo in caso di incidente*
  - *Effettuare Test di efficacia*



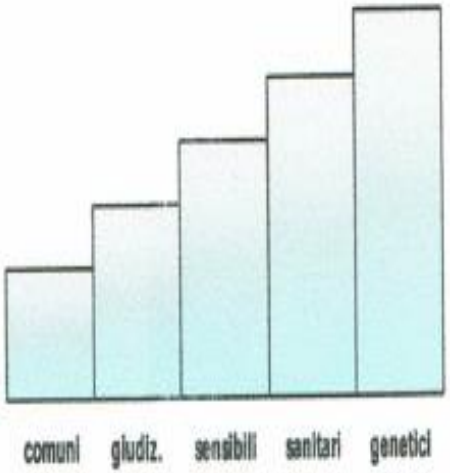
- **OTTICA DA SEGUIRE**
  - ***Proteggere la privacy*** *e non (solo) la sicurezza del patrimonio aziendale*

La Sicurezza Del Trattamento
IL LIVELLO DI SICUREZZA

QUALITA' DELLE MISURE

- *Livello di protezione "ADEGUATO"*
- *Tenuto conto di*
  - *Stato dell'arte e sviluppi tecnici*
  - *Natura dei dati,*
  - *Contesto e strumenti adottati*
  - *Probabilità e gravità dei rischi.*
  - *Bilanciamento costi vs rischi*

New



MONITORAGGIO

- *Livello di "adeguatezza" delle misure, in continua evoluzione*

La Sicurezza Del Trattamento
COPERTURA

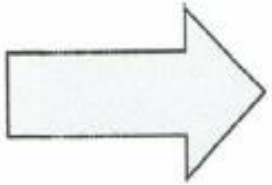
- **PRIMA DI INIZIARE IL TRATTAMENTO**

- **DURANTE TUTTE LE OPERAZIONI DI TRATTAMENTO**
  - *Raccolta, conservazione, trasmissione, elaborazione ...*

- **QUALUNQUE SIA LO STRUMENTO / MODALITA'**
  - ***Elettronici:*** *server centralizzati, cloud, informatica individuale, PC, smartphon, tablet, etc...*
  - ***Cartacei***
  - ***Altro:*** *fax , stampanti ...*

La Sicurezza Del Trattamento
COMPORTAMENTO DEI DIPENDENTI

- **PREVENIRE ILLECITA DIVULGAZIONE**
  - *A Terzi*
  - *A Colleghi: Principio del Need to Know*
  - *Clean Desk Policy*
- **PROTEGGERE DATI vs STRUMENTI**
  - *Segretezza e robustezza Psw, utilizzo PIN*
  - *Screen saver,*
  - *Controllo e custodia degli strumenti*
- **PROTEGGERE DATI vs LUOGHI/ACQUISIZIONI INVOLONTARIE**
  - *Distanze di cortesia/ Open Space/Aree chiuse*
  - *Presidio Stampanti, Copiatrici, Fax ...*
  - *Separazione dati sensibili da dati comuni*
  - *Distruggi documenti*



CONSAPEVOLEZZA/FORMAZIONE

La Sicurezza Del Trattamento
AZIONI E DOCUMENTAZIONE

- **AMBITI DI INTERVENTO**
  - *Logici*
  - *Tecnici e di sicurezza fisica*
  - *Organizzativi e procedurali*
  - *Di processo*
  - *Di Formazione / Informazione*
  - *Audit*

New

- **ACCOUNTABILITY**
  - *Obbligo di documentare e fornire prova*

New

- **POSSIBILI SEMPLIFICAZIONI PER PMI**
  - *Adesione a Codici Condotta art 40, Cerificazione art 39*

Misure di Sicurezza Adeguate – Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati

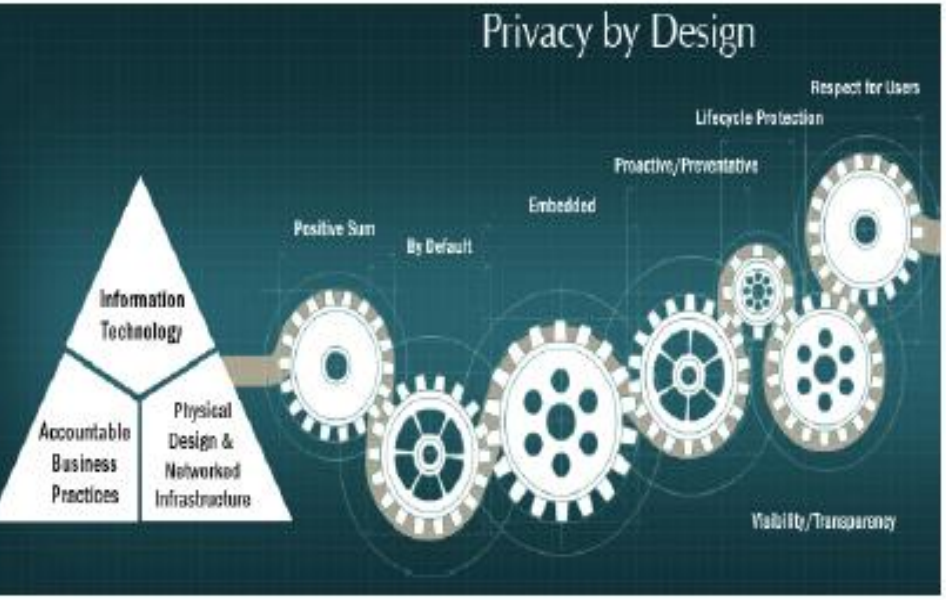
Divulgazione non autorizzata dei Dati

Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Privacy By Design e By Default – Art. 25

in dalla progettazione bisogna prevedere che le misure volte alla protezione dei dati personali
ano integrate nell'intero ciclo di vita tecnologico, dalla primissima fase di ideazione fino alla sua
ealizzazione, al suo utilizzo ed allo smaltimento finale.



Privacy By Design:
Individuazione di misure tecniche e organizzative adeguate per la protezione dei dati, già durante la fase di progettazione

Privacy By Default:
Garantire che siano trattati di default solo i dati personali necessari per ogni specifica finalità del trattamento

Pseudonimizzazione

Minimizzazione

Minimizzazione

Limitazione delle finalità

Integrazione delle garanzie a tutela dei diritti degli Interessati

Si potrà utilizzare un meccanismo di certificazione approvato per dimostrare la conformità del processo a tali requisiti.

New

REGISTRO DEI TRATTAMENTI- art 30

Obbligo di documentazione

CHI E' OBBLIGATO

- *il Titolare e anche il Responsabile*

IN COSA CONSISTE

- *Un Registro delle attività di trattamento in forma scritta anche elettronica:*
- *A disposizione del Garante*

COSA DEVE CONTENERE

- *Quadro di Censimento e di sintesi: Nome del Titolare (o del Responsabile e del Titolare per cui si agisce) Descrizione delle attività effettuate dal Titolare (o per conto del Titolare), Finalità, Categorie dei dati, Destinatari dei dati, Misure di sicurezza adottate, Termini per la cancellazone dei dati, Destintari extra UE e loro misure di garanzia ...*

ECCEZIONI ESTREMAMENTE LIMITATE

- *Non applicabile < 250 dipendenti a meno che :*
  - ✓ *il trattamento non sia occasionale, includa "dati particolari" o possa provocare rischi per diritti e libertà degli interessati,*

Simil DPS- assegnazione compito a struttura per gestione e aggiornamento

Registro delle attività di trattamento - Art. 30

Il Registro delle Attività di Trattamento (**PRIVACY BOOKING**) sarà un documento di tipo dinamico ed una sorta di memoria storica dell'azienda in materia di sicurezza dei Dati.

Nome e contatti di ogni Responsabile (esterni e interni)

Finalità di Trattamento

Categorie di Interessati e di Dati trattati

Categorie di destinatari a cui i dati sono comunicati

Informazioni sui trasferimenti verso paesi terzi

Termini per la cancellazione dei dati

Misure di sicurezza tecniche e organizzative

Backup & Recovery

Reg. Informatico

Policy e Procedure

Formazione

Registro delle attività di trattamento – Art. 30

Il Registro delle Attività di Trattamento (Privacy Booking) sarà un documento di tipo dinamico ed una sorta di memoria storica dell'azienda in materia di sicurezza dei Dati.

Nome e contatti di ogni Responsabile (esterni e interni)

Finalità di Trattamento

Categorie di Interessati e di Dati trattati

Categorie di destinatari a cui i dati sono comunicati

Informazioni sui trasferimenti verso paesi terzi

Termini per la cancellazione dei dati

Misure di sicurezza tecniche e organizzative

Backup & Recovery

Reg. Informatico

Policy e Procedure

Formazione

Registro delle attività di trattamento – Art.

Gli obblighi di cui all'Art.30 non si applicano alle aziende con meno di **250 dipendenti**, tran
seguenti casi:

Trattamento con rischi per diritti e libertà dell'Interessato

Trattamento non occasionale dei dati

Trattamento di categorie particolari di dati

Trattamento di dati relativi a condanne penali e reati

Data Breach Notification – Art. 33

Liberi PROFESSIONISTI
www.professionistiliberi.org

Nel caso in cui si verifichi una violazione di dati personali, il Titolare del Trattamento ha l'Obbligo di Notifica, che dovrà essere eseguito sia ai diretti interessati, che all'Autorità Garante per la protezione dei dati personali, entro ~~24 ore~~ 72 ore. Attualmente in Italia tale obbligo trova applicazione per le sole organizzazioni che forniscono servizi di comunicazione elettronica.

Soggetti Interessati

Autorità Garante

~~Conservazione Registro Pubblico delle tipologie di violazioni notificate~~

La decorrenza delle 72 ore parte dal momento in cui il Titolare viene a conoscenza della violazione, a meno che sia improbabile che essa presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora non siano rispettate tali tempistiche, la notifica all'Autorità Garante va corredata da una giustificazione motivata.

Data Breach Notification – Art.33

La comunicazione all'Interessato non è richiesta nei casi di:

Utilizzo di misure tecniche e organizzative adeguate per rendere i dati incomprensibili ai soggetti non autorizzati (cifratura)

Successiva adozione di misure atte a scongiurare il sopraggiungere di rischi per i diritti e le libertà degli interessati

Comunicazione particolarmente difficoltosa o onerosa per il Responsabile

In questo caso occorre procedere a comunicazione pubblica o misura simile

Data Protection Officer – Art. 37

Il Data Protection Officer, che potrà essere interno od esterno all'organizzazione, avrà il compito di progettare e mantenere un sistema organizzato e sicuro di gestione dei dati personali. Tale figura dovrebbe poter adempiere alle proprie funzioni in maniera indipendente.

Per chi sarà Obbligatorio?

Pubblica Amministrazione
Molto più di un'icona.

Pubbliche Amministrazioni

~~Grandi Aziende Private (oltre 250 dipendenti)~~

In Caso di Trattamento di Dati di ~~più di 5.000~~ Interessati su larga scala

In Caso di Trattamento di Dati Particolari su larga scala

Facoltatività per ciascuno Stato membro di introdurre la figura del DPO come obbligatoria.

Enti pubblici o gruppi d'imprese possono nominare un unico DPO per più stabilimenti/autorità.

I Compiti del DPO – Art. 39

Informare e consigliare Titolare, Responsabili e dipendenti

Sorvegliare l'attuazione e l'applicazione del Regolamento

Sorvegliare l'attuazione e l'applicazione delle politiche aziendali

~~Garantire la conservazione del Registro delle Attività di Trattamento~~

~~Controllare che le violazioni dei dati siano notificate~~

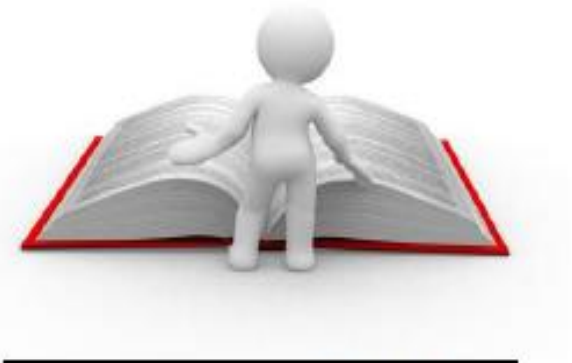
Verificare e fornire un parere sulla valutazione d'impatto

Cooperare con l'Autorità di controllo

Fungere di punto di contatto tra l'Autorità e gli Interessati

Il DPO opera considerando i rischi inerenti al trattamento, tenendo conto della relativa natura, campo di applicazione, contesto e finalità.

Le Competenze del DPO – Art. 37



Conoscenza Specialistica della Normativa

Conoscenza delle Pratiche in materia di Protezione dei Dati

Adempiere ai Compiti dell' Art. 39

Padronanza Requisiti Tecnici

Specifica Conoscenza del Settore

Analisi, Audit e Consultazioni

Collaborazione e Spiccate Capacità Relazionali

Formazione Avanzata Specializzata

Questi requisiti minimi era presenti in modo esplicito soltanto nel testo del Parlamento Europeo (75 bis). Nel testo definitivo si fa riferimento solo alle tre competenze riportate in alto.

Il DPO è una figura autonoma e indipendente dall'organizzazione e riferisce direttamente al vertice gerarchico.

New

Il Data Protection Officer Art 37-39 (1/4)

ADERISCO Liberi PROFESSIONISTI www.professionistiliberi.org

NUOVA CATEGORIA PROFESSIONALE

- *Figura di Garanzia Aggiuntiva interna all'Azienda*
- *Diversa dal Responsabile del trattamento e dal Compliance Manager*

CHI E' OBBLIGATO A NOMINARLO

- *Il Titolare e il Responsabile*

QUANDO E' OBBLIGATORIA LA NOMINA

- *Enti Pubblici*

- *Privati - Quando le attività principali consistono:*

  - ✓ *Trattamenti che per loro natura, ambito di applicazione e/o finalità richiedono il monitoraggio regolare e sistematico di interessati su larga scala,*

    oppure

  - ✓ *Trattamento su larga scala di "dati particolari" o "dati "penali"*

New

Il Data Protection Officer (2/4)

ADERISCO Liberi PROFESSIONISTI www.professionistiliberi.org

- **REQUISITI**
  - ***PROFESSIONALITA':*** *Qualità professionali, conoscenze giuridiche, informatiche ...*
  - ***ESPERIENZA:*** *Competenza specialistica di normativa e pratiche privacy*
  - ***CAPACITA':*** *di assolvere i Compiti previsti dall'art 39 del Regolamento*

- **CHI PUO' RICOPRIRE IL RUOLO**
  - *Dipendente del Titolare o del Responsabile*
  - *oppure*
  - *Un Esterno con "contratto di servizi"*

New

Il Data Protection Officer (3/4)

- **CONOSCIBILITA'**
  - *Dati di contatto comunicati al Garante*
  - *Indicati nell'Informativa*
- **GARANZIE**
  - *Deve essere tempestivamente e adeguatamente coinvolto nelle questioni privacy*
  - *Supportato con le risorse necessarie a svolgere i compiti*
  - *Indipendente e autonomo nel ruolo. Non deve ricevere istruzioni*
  - *Riferisce direttamente al vertice gerarchico*
  - *Può essere contattato direttamente dagli interessati*
  - *Può svolgere altri incarichi purchè no conflitto di interessi*
  - *Non può essere rimosso per l'adempimento dei propri compiti*

New

Il Data Protection Officer (4/4)
COMPITI

"Piccolo Garante" in Azienda

- **INFORMAZIONE E CONSULENZA**
  - Al Titolare, al Responsabile , agli Incaricati in merito ai loro obblighi
- **SORVEGLIANZA**
  - In merito all'osservanza del Regolamento e delle Policies aziendali e l'attribuzione delle responsabilità;
    - ✓ quindi: il rispetto dei diritti dell'interessato Informativa, Consenso, Accesso ai dati/ delle Misure di sicurezza/ della Notifica delle violazioni/ del principio di privacy by design/ della valutazione di impatto / della conservazione della documentazione, l'effettuazione dei controlli...)
  - Sensibilizza il personale e ne cura la formazione, inclusi gli auditors
- **SUPPORTO E INDIRIZZO**
  - Fornisce, se richiesto, parere in merito alla Valutazione di Impatto e ne sorveglia il seguito
- **RELAZIONI CON ESTERNO**
  - Coopera col Garante: le sue coordinate devono essere notificate
  - Punto di contatto con gli Interessati- coordinate nell'Informativa

ADERISCO Liberi PROFESSIONISTI www.professionistiliberi.org

LE SANZIONI

QUADRO SANZIONATORIO AMMINISTRATIVO MUTATO

SANZIONI PENALI CONFERMATE E MODIFICATE

INTRODUZIONE NUOVE SANZIONI PENALI DA D.LGS 101/2018

LE VIOLAZIONI DELLA PRIVACY E IL SISTEMA SANZIONATORIO- art 77 segg

SANZIONE AMMINISTRATIVA

RISARCIMENTO DANNI

SANZIONE PENALE

DANNO DI IMMAGINE

LE SANZIONI AMMINISTRATIVE

- **AUTORITA' CHE LE INFLIGGE**
  - *Garante della Privacy*
- **SORGENTE**
  - *A seguito di indagini*
  - *A seguito di reclami*
- **CONTENUTO**
  - ***In casi lievi :*** *avvertimento, ammonimento*
  - ***Altro:*** *ingiunzione, inibizione del trattamento, sanzione pecuniaria*
- **OPPOSIZIONE**
  - *Ammesso ricorso all'A.G. contro decisione Garante*

Sanzioni – Art. 84

Il testo di Regolamento Europeo, rafforzato dal Parlamento Europeo, prevede sanzioni amministrative pecuniarie particolarmente elevate, anche proporzionate al volume di affari realizzato da una società, e dissuasive soprattutto per i Big Data.

Fino a 10.000.000 di € o

del fatturato mondiale annuo

- Violazioni degli obblighi del Responsabile e dell'Incaricato del Trattamento
- Violazione degli obblighi dell'organismo di certificazione
- Violazione degli obblighi dell'organismo di controllo

Fino a 20.000.000 di € o

del fatturato mondiale annuo

- Mancata osservanza di un ordine da parte dell'Autorità di controllo
- Violazione di nome su consenso, trasferimento verso paesi terzi e diritti degli interessati
- Mancata osservanza di leggi degli Stati membri

Il legislatore prevede un avvertimento scritto o una serie di verifiche periodiche presso il Responsabile, qualora questi abbia violato le norme per la prima volta e in caso di semplice colpa.

Le Sanzioni Amministrative
PECUNIARIE

New **PRINCIPI GENERALI**

- *Deve essere: effettiva, proporzionata, dissuasiva*

New **VALORE**

- *Notevolmente rafforzato*
- *Fino a 20 Milioni di euro*

o

- *Fino al 4% del Fatturato mondiale /anno precedente*

New **CRITERI**

- *Natura e gravità , durata*
- *Carattere intenzionale o colposo*
- *Recidività*
- *Altre aggravanti,/ attenuanti*

IL RISARCIMENTO DEL DANNO- art 82

- **CHI PUO' CHIEDERE IL RISARCIMENTO**
  - *Chiunque abbia subito un danno: Interessato o terzo*
- **COSA PUO' CHIEDERE**
  - *Danni patrimoniali*
  - *Danni non patrimoniali*
- **A CHI DEVE RIVOLGERSI**
  - *All'Autorità Giudiziaria.*
- **CONTRO CHI**
  - *Titolare o Responsabile autore della violazione*
- **ESONERO DA RESPONSABILITA'**
  - *Evento dannoso non imputabile*

New

SANZIONI PENALI –art 84

- **REGOLAMENTO UE**
  - *Non le contempla direttamente*
  - *Rimanda a leggi nazionali degli Stati membri*

- **LEGGI NAZIONALI**
  - *Pene detentive*
  - *Sottrazione profitti*

INADEMPIMENTO	D.Lgs n. 101/2018
Omessa o inidonea informativa All'interessato. (Art. 161)	ABROGATO
Assenza informativa nei casi di dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilev	ABROGATO
Omessa o incompleta notificazione al Garante Privacy. (Art.163)	ABROGATO
Omessa informazione o esibizione di documenti richiesti dal garante Privacy. (Art.164)	ABROGATO
Trattamento illecito di dati personali. (Art. 167 c.1.)	**Reclusione da 6 mesi a 1 anno e 6 mesi**. La pena è diminuita se il Garante ha riscosso la sanzione amministrativa
Trattamento illecito di dati personali. (Art. 167 c.2)	**Reclusione da 1 a 3 anni**. La pena è diminuita se il Garante ha riscosso la sanzione amministrativa. .
Trattamento illecito di dati personali. (Art. 167 bis c.1) *(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*	**Reclusione da 1 a 6 anni.**

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è **punito con la reclusione da sei mesi a un anno e sei mesi.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al rattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-*sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2- septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2- quinquiesdecies arreca nocumento all'interessato****, è punito con la reclusione da uno a*** **tre anni.**

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli
- 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
- 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

CAPO III – Illeciti Penali

Art. 167 - *bis* (*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*

- 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-*ter, 2-sexies e 2-octies, è punito* **con la reclusione da uno a sei anni.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, **è punito con la reclusione da uno a sei anni,** quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

CAPO III – Illeciti Penali
Art. 167–*ter*(*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)*

c.1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è pun**ito con la reclusione da uno a quattro anni.**

1 a 4 anni

CAPO III – Illeciti Penali

Art. 168 (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)*

C 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con **la reclusione da sei mesi a tre anni.**

C 2. Fuori dei casi di cui al comma 1, è punito con la **reclusione sino ad un anno** chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

CAPO III – Illeciti Penali
Art. 170 (*Inosservanza di provvedimenti del Garante)*

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

3 mesi a 2 anni

Reati informatici

- Reati compiuti per mezzo o nei confronti di un sistema informatico. L'illecito può consistere nel sottrarre o distruggere le informazioni contenute nella memoria del personal computer. In altri casi, invece, il computer concretizza lo strumento per la commissione di reati, come nel caso di chi utilizzi le tecnologie informatiche per la realizzazione di frodi. La prima normativa contro i cyber crimes L. 547/1993:

- Frode informatica (art. 640): consiste nell'alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto (Phishing)
- Accesso abusivo a un sistema informatico o telematico (art. 615 ter) : condotta di colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontàdi chi ha il diritto di escluderlo o violando le prescrizioni del titolare del sistema.
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 614 quater c.p.) : al fine di procurare a sé o ad altri un profitto o di arreca ad altri un danno, riproducendo, diffondendo, comunicando o consegnando codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni idonee

-

Reati informatici

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies) chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione.
- Intercettazione, impedimento o interruzione illecita di comunicazioni (artt. 617 quater e 617 quinquies) chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui che installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni informatiche.
- Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi (art. 617 sexies) Chi falsifica, altera o sopprime la comunicazione informatica acquisita e chi distrugge, deteriora, cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.).
-

Question Time


grazie