



CONFCOMMERCIO COMO
IMPRESE PER L'ITALIA

UNIONE PROVINCIALE COMMERCIO TURISMO SERVIZI

Privacy

La situazione attuale

D.Lgs. n.196/2003

Como, 7 maggio 2018



DATO PERSONALE

qualunque informazione relativa a persona fisica identificata o identificabile

DATO SENSIBILE

dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati...nonché a rivelare lo stato di salute e la vita sessuale



TRATTAMENTO

qualunque operazione concernente la raccolta, la registrazione, la conservazione, la consultazione, l'elaborazione, la modificazione...., la comunicazione, la diffusione...



IL TRATTAMENTO E' CONSENTITO SE:

- ✓ effettuato in modo **lecito** (es. obbligo di legge, esecuzione contratto, consenso) e secondo correttezza
- ✓ per scopi determinati, **espliciti** e legittimi
- ✓ i dati trattati sono **pertinenti** e non eccedenti le finalità per le quali sono raccolti
- ✓ relativo a **dati esatti**



L'INTERESSATO DEVE ESSERE INFORMATO circa:

- ✓ **finalità**, modalità e natura del trattamento
- ✓ conseguenza del rifiuto
- ✓ soggetti a cui possono essere **trasferiti** i dati
- ✓ identificazione del **Titolare** del trattamento
- ✓ i **diritti** di cui gode (art.7 D.Lgs. n.196/2003)

L'informativa può essere ORALE o SCRITTA



IL CONSENSO AL TRATTAMENTO NON E' RICHIESTO SE:

- ✓ è necessario per adempiere ad un obbligo di legge
- ✓ è necessario per adempiere ad obblighi derivanti da un contratto di cui è parte l'interessato
- ✓ riguarda dati provenienti da pubblici registri, elenchi, atti ecc.

Ma per i **DATI SENSIBILI** il consenso scritto è
SEMPRE necessario



GLI OBBLIGHI

- ✓ **TRATTARE** i dati in modo **LECITO**
- ✓ **INFORMARE** del trattamento il titolare dei dati
- ✓ avere il consenso al trattamento nel caso di dati sensibili
- ✓ garantire la **SICUREZZA** dei dati trattati (perdita, diffusione, accesso improprio, trattamento non lecito, ecc.)
- ✓ **INDIVIDUARE** i legittimi incaricati al trattamento

RGPD EU 679/2016

Regolamento Generale sulla Protezione dei Dati

Como
7 Maggio 2018
Auditorium Opera don Guanella

Legislazione di Riferimento ed Evoluzione Normativa



CONFCOMMERCIO COMO
IMPRESE PER L'ITALIA
UNIONE PROVINCIALE COMMERCIO TURISMO SERVIZI

ASSOPRIVACY****

Direttiva Europea 46/1995 CE



D. Lgs. 675/1996



Testo Unico D. Lgs. 196/2003



**Regolamento Europeo (UE) 2016/679
(dal 25 Maggio 2018)**

Lex 25 ottobre 2017 n. 163 di delegazione europea 2016-2017

Trattamento dei Dati Personali

con o senza l'ausilio di strumenti elettronici

- ☐ **raccolta dei dati**
- ☐ **registrazione – organizzazione - conservazione**
- ☐ **consultazione**
- ☐ **elaborazione**
- ☐ **blocco**
- ☐ **modificazione**
- ☐ **utilizzo**
- ☐ **interconnessione, comunicazione, diffusione**
- ☐ **cancellazione, distruzione**
- ☐ **selezione, estrazione, raffronto**

Dati Personali

tutte le informazioni relative a persone fisiche che consentano l'identificazione diretta o indiretta di questi stessi soggetti

- ❑ **Dati comuni**, anagrafici ed economici, anche immagini, suoni e i codici identificativi riconducibili a un individuo (Fotografie - Telecamere – Dipendenti - Ospiti – Social Networks).
- ❑ **Dati Particolari (Sensibili)**, attinenti alla sfera personalissima dei singoli (informazioni sulle opinioni religiose o politiche, sulle abitudini sessuali, sullo stato di salute, etc.), per i quali la legge prevede una tutela più forte rispetto agli altri (Dati Alimentari – Religiosi – Preferenze – Profilazione).
- ❑ **Dati Giudiziari**, relativi a procedimenti, trattamento ammesso solo se autorizzato da espressa disposizione di legge (o provvedimento del Garante), che ne specifichi le finalità, i tipi di dati e le operazioni autorizzate, che preveda garanzie appropriate per i diritti e le libertà degli interessati, sotto il controllo dell'autorità pubblica.

Soggetti del Trattamento

- ☐ Il Titolare - Contitolari
- ☐ Il Responsabile (Interno – Esterno)
- ☐ L'Incaricato
- ☐ L'Interessato
- ☐ Il DPO Responsabile della Protezione dei Dati
- ☐ Rappresentante di Titolari del Trattamento o dei Responsabili del Trattamento non stabiliti nell'Unione

Riepilogo Generale Obblighi Codice Privacy Attuale

1. **Designazioni Incaricati e Formazione degli Stessi** per istruirli sulla Sicurezza;
2. **Informative** ex art 13 per ogni finalità;
3. **Rilevazione del Consenso** Informato per ogni finalità;
4. **Assicurare Esercizio Diritti art. 7 (15 e ss GDPR)** all'interessato;
5. **Implementazione Struttura informatica** protetta che sia in linea con l'evoluzione tecnologica;
6. **Misure (*Minime*) di Sicurezza** Logistico – Informatiche;
7. Riscontro alle Richieste Authority;
8. Rispetto Normative Connesse: Lex 300/70;
9. **Rispetto Provvedimento del 2008 sui log** per accessi degli Amministratori Sistema;
10. **Rispetto altri Provvedimenti Emessi dall'Authority** (modifiche legislative permettendo).

Impianti di Audio – Video Registrazione

- ❑ Provvedimento del Garante per la Protezione dei Dati Personali dell'8 Dicembre 2010;
- ❑ Statuto dei Lavoratori ex art. 4 Lex 300/70 (divieto Controllo a Distanza):
 - accordo con le Rappresentanze Sindacali, se presenti;
 - in mancanza - **autorizzazione Ispettorato Territoriale del Lavoro competente**

Informazioni da fornire agli Interessati – art. 13

- ☐ le finalità del trattamento;
- ☐ l'obbligo o la facoltà di conferire i dati;
- ☐ le conseguenze giuridiche del rifiuto a rispondere;
- ☐ i soggetti a cui i dati possono essere comunicati;
- ☐ l'ambito di diffusione dei dati personali;
- ☐ i diritti spettanti al soggetto interessato;
- ☐ identificazione del titolare del trattamento, del responsabile nel territorio dello Stato, di almeno un responsabile del trattamento;
- ☐ *Tempi o Criteri di Conservazione;*
- ☐ *Trasferimento dati extra EU;*
- ☐ *Indicazione contatto DPO;*
- ☐ *Diritto di Proporre Reclamo;*
- ☐ *Diritti (accesso - oblio - portabilità);*
- ☐ *L'esistenza di un processo decisionale automatizzato - compresa la profilazione.*

Consenso – Liceità del Trattamento

Regola Generale: *Necessario*

- ❑ Il trattamento di dati personali è ammesso soltanto con il Consenso Informato dell'interessato, ed è validamente prestato soltanto se è espresso liberamente. Il Consenso deve essere in ogni caso
 - documentabile;
 - specifico;
 - Inequivocabile.

Non Necessario se

- ❑ per adempiere ad obblighi previsti da leggi;
- ❑ per l'esecuzione di un contratto di cui è parte l'interessato;
- ❑ per perseguire un legittimo interesse del titolare anche in riferimento all'attività di gruppi bancari e di società controllate o collegate : Esempio = Videosorveglianza;
- ❑ effettuato da associazioni, enti o organismi senza scopo di lucro, per il raggiungimento di scopi determinati e legittimi.

Regolamento Generale Protezione Dati UE 2016/679

❑ Nuovi Adempimenti :

- Attività di *Data Protection Impact Assessment* - Valutazione d'Impatto sulla protezione dei dati - **eventuale**;
- *Data Breach* - *Violazioni dei Dati* - *Obbligo di Notifica*
- Diritto alla Portabilità dei Dati;
- Diritto all'Oblio – Revoca del Consenso;
- Informative Chiare e Trasparenti sui Trattamenti;
- Titolare e Responsabile del Trattamento;
- Principio di Rendicontazione “Accountability» - artt. 24 e 32;
- *Privacy by Design e by Default* “*Progettazione e Necessarietà*” - art. 25
- Modalità e Tenuta del Registro dei Trattamenti - art. 30 - **eventuale**;
- Introduzione della figura del Data Protection Officer - **eventuale**;
- One-stop-shop – Trattamenti Transfrontalieri Intra EU – *Lead Authority*;
- Sanzioni amministrative (art. 83) 20 Mln Euro o 4% Fatturato Globale

Responsabile del Trattamento – art. 28

- ❑ Responsabili: **Interni ed Esterni**
- ❑ **Esterni**: Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
- ❑ I trattamenti da parte di un responsabile del *trattamento* sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento
- ❑ Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento (previa autorizzazione scritta) per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto, gli stessi obblighi in materia di protezione dei dati contenuti nel tra il titolare del trattamento e il responsabile del trattamento.
- ❑ Il contratto o altro atto giuridico di cui ai paragrafi precedenti è stipulato in forma scritta, anche in formato elettronico.

Responsabile della Protezione dei Dati – art. 37 (DPO)

- ❑ ***Figura non contemplata nella attuale legislazione***
- ❑ Il Titolare o il Responsabile del Trattamento dei Dati Personali debbono designare un RDP (Responsabile della Protezione dei Dati Personali o DPO - Data Protection Officer) ogni qualvolta:
 - il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico.
 - le attività principali del Titolare o del Responsabile consistano in trattamenti che, per loro natura, campo di applicazione e/o finalità richiedano il controllo regolare e sistematico degli interessati su larga scala;
 - il Titolare o il Responsabile trattino, **su larga scala dati particolari (sensibili e/o giudiziari)**.
- ❑ L'RDP dovrà svolgere *i suoi precisi compiti in autonomia e sarà dotato delle risorse necessarie per assolvere ai suoi compiti*. Egli riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
- ❑ Un gruppo imprenditoriale può nominare **un unico responsabile** della protezione dei dati.
- ❑ Può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Nei casi più complessi questa figura può essere rappresentata da un pool di esperti in materia.
- ❑ Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un **conflitto di interessi**.

Responsabile della Protezione dei Dati – art. 37 (DPO)

- ❑ L'RDP deve essere designato in base alla sua comprovata professionalità e, in particolare, alla sua conoscenza specialistica della legislazione europea della protezione dei dati e della prassi in materia ed è tenuto, tra le altre cose a:
 - informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Nuovo Regolamento e da altre disposizioni dell'UE.
 - sorvegliare che il Nuovo Regolamento sia osservato;
 - fornire un parere in merito alla Valutazione d'Impatto (DPIA);
 - cooperare con l'autorità di controllo (Garante Privacy);
 - assicurare l'esercizio dei diritti degli interessati.

- ❑ L'RDP, per comprovare nel tempo al sua professionalità, dimostra di avere innanzitutto esperienza storica in materia e, successivamente, di aver effettuato dei corsi professionali e di aggiornamento periodici possibilmente certificati.

Principio di Rendicontazione - artt. 24 e 32

- ❑ Sono ridefinite le responsabilità del Titolare e Responsabile del Trattamento dei Dati attribuendo loro obblighi ulteriori. La non concretezza e l'inefficienza delle policy di sicurezza e protezione previste costituisce per il Titolare fonte di responsabilità (principio di Rendicontazione o di "Accountability").
- ❑ Tenendo conto dello stato dell'arte e del rischio di gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, **tra le altre, se del caso**:
 - la **pseudonimizzazione** e la **cifratura** dei dati personali;
 - la capacità di **assicurare la riservatezza, l'integrità**, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
 - la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - una **procedura per testare**, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- ❑ Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi 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.

Privacy by Design e by Default - art. 25

- ❑ Il Titolare deve adottare e attuare misure tecniche e organizzative sin dal momento della progettazione di un determinato trattamento (by Design) oltre che nella fase della sua esecuzione, mirate a tutelare i principi di protezione dei dati.
- ❑ Inoltre nell'operatività il Titolare deve adottare, per impostazione predefinita (by Default), misure tecniche che garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

Obbligo di Comunicazione di Violazione di Dati Personali - artt. 33 e 34

- ❑ Il Titolare e il Responsabile devono comunicare l'eventuale avvenuta Violazione di Dati Personali (Data Breach), quali che siano i trattamenti posti in essere, *(caso rilevante anche e soprattutto per le conseguenze sul piano giuridico e i rischi derivanti sulla sicurezza come la perdita o compromissione di dati nonché il danneggiamento della reputazione aziendale / professionale)*.
- ❑ Il Responsabile ha l'obbligo di informare il Titolare della eventuale violazione senza ingiustificato ritardo e quest'ultimo, a sua volta, deve notificare la violazione, senza ingiustificato ritardo, all'autorità Garante. È previsto, inoltre, un **obbligo di comunicazione anche all'interessato**, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Valutazione d'Impatto sulla protezione dei dati - art. 35

- ❑ quando un determinato trattamento - tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare un (Data Protection Impact Assessment-'DPIA') ossia una Valutazione d'Impatto sulla protezione dei dati, in collaborazione con il RDP.
- ❑ la Valutazione d'Impatto deve contenere la descrizione dei trattamenti previsti e delle finalità, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità e una valutazione per i rischi per i diritti e le libertà degli interessati come le misure previste per affrontare i rischi.
- ❑ la Valutazione d'Impatto è richiesta in particolare nei seguenti casi:
 - quando avviene una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la Profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono su dette persone fisiche;
 - quando si effettua un trattamento su larga scala di dati sensibili e giudiziari;
 - quando si effettua una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Registri delle Attività di Trattamento - art. 30

- ❑ Il Titolare e il Responsabile del Trattamento devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente tutti gli specifici elementi di cui all'art. 30 del Nuovo Regolamento.
- ❑ L'obbligo di tenuta dei registri non si applica in linea di principio alle imprese o organizzazioni con meno di 250 dipendenti, a meno che si preveda il trattamento di dati **sensibili** e/o **giudiziari**, sia occasionale o possa rappresentare un rischio per i diritti e le libertà dell'interessato.

Nuovi Diritti per l'Interessato

- ❑ **Diritto all'oblio** (art. 17). Evoluzione dell'attuale diritto alla cancellazione, è il diritto del singolo interessato ad essere "dimenticato" dalle banche dati, dai mezzi di informazione, o dai motori di ricerca su base legislativa del Diritto all'Oblio.

Consiste nel diritto di chiedere che siano cancellati i suoi dati personali che non siano più necessari per le finalità per le quali sono stati raccolti, da cui abbia ritirato il consenso al trattamento, si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme alla legge.

- ❑ **Portabilità dei dati** (art. 20) L'interessato ha inoltre il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al Titolare, e di trasmettere i propri dati da un Titolare (ad esempio un social network) ad un altro Titolare (Data Portability), senza impedimenti da parte di colui al quale sono stati forniti in precedenza.

- ❑ **Soggetti Interessati:**

- Titolare del Trattamento;
- Responsabile del Trattamento;
- Responsabili Esterni del Trattamento;
- Responsabile della Protezione dei Dati Personali (DPO).

Sanzioni Privacy

Causa	Sanzione Amministrativa		Sanzione Penale		Riferimento Normativo
	Minima	Massima	Minima	Massima	
Informativa Omessa o Irregolare	€ 6.000,00	€ 36.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 161
Cessione Dati a Terzi	€ 10.000,00	€ 60.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 162 - 1
Comunicazione Dati Sanitari Irregolare	€ 1000,00	€ 6.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 162 - 2
Violazione Disposizioni per Conservazione Dati di Traffico Telematico	€ 10.000,00	€ 120.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 162 Bis
Notificazione Omessa o Incompleta	€ 20.000,00	€ 120.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 163
Omesse Informazioni o Esibizioni al Garante	€ 10.000,00	€ 60.000,00 + Pubblicazione Sentenza			D. Lgs 196/03 Art. 164
Trattamento Illecito Dati	€ 20.000,00	€ 120.000,00	Reclusione da 6	a 24 mesi + Pubblicazione Sentenza	D. Lgs 196/03 Artt. 162 - 2 bis - 167
Falsità Comunicazioni al Garante			Reclusione da 6	a 36 mesi + Pubblicazione Sentenza	D. Lgs 196/03 Artt. 161 - 168
Omissione Misure Minime Sicurezza	€ 10.000,00	€ 120.000,00	o Reclusione	Sino a 24 mesi + Pubblicazione Sentenza	D. Lgs 196/03 Artt. 162 - 2 bis - 169
Inosservanza Provvedimenti Garante	€ 30.000,00	€ 180.000,00	Reclusione da 3	a 24 mesi + Pubblicazione Sentenza	D. Lgs 196/03 Artt. 161 - 162-ter - 170
Raccolta dei Dati e Controllo a Distanza	€ 150,00	€ 7.500,00	+ Reclusione da 15 gg	a 1 anno + Pubblicazione Sentenza	D. Lgs 196/03 Art. 171 -Lex 300/70 Art. 38
Informativa Omessa o Irregolare Codice Consumo	€ 3.000,00	€ 18.000,00			D. Lgs 20/05 Art. 62
Violazione del Regolamento Europeo		€ 20 Milioni / 4% FT			GPDR 679/2016 Art. 83



Como

7 Maggio 2018

Il nuovo Regolamento europeo Privacy

**GDPR: General Data Protection Regulation
(Reg. UE n. 2016/679)**

GDPR is coming...



Cosa cambia*

**Imprese ed enti avranno
più responsabilità, ma potranno
beneficiare di semplificazioni.
In caso di inosservanza delle regole
sono previste sanzioni,
anche elevate.**

*Fonte: Garante Privacy

Applicabilità

Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea.

Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

Accountability e risk management



**Approccio basato
sulla valutazione
del rischio che
premia i soggetti
più responsabili**

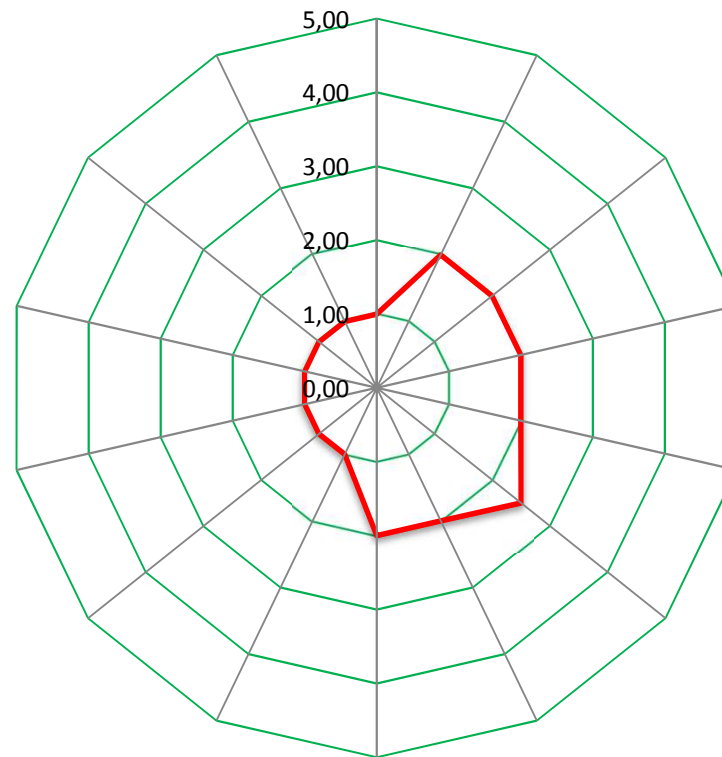


Accountability

(Documentare la conformità al GDPR)

- ✓ Sono ridefinite le responsabilità del Titolare e Responsabile del Trattamento dei Dati attribuendo loro obblighi ulteriori. La non concretezza e l'inefficienza delle policy di sicurezza e protezione previste costituisce per il Titolare fonte di responsabilità (principio di Rendicontazione o di "Accountability").
- ✓ Tenendo conto dello stato dell'arte e del rischio di gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - ✓ la pseudonimizzazione e la cifratura dei dati personali;
 - ✓ la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
 - ✓ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - ✓ una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- ✓ Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi 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.

Risk Assessment



Privacy by design

Il principio-chiave è «*privacy by design*», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.



Privacy by design

- ✓ Il Titolare deve adottare e attuare misure tecniche e organizzative sin dal momento della progettazione di un determinato trattamento (by Design) oltre che nella fase della sua esecuzione, mirate a tutelare i principi di protezione dei dati.
- ✓ Inoltre nell'operatività il Titolare deve adottare, per impostazione predefinita (by Default), misure tecniche che garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

D.P.I.A.

Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi.



D.P.I.A.

Data Protection Impact Assessment

- ✓ Quando un determinato trattamento - tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare un (Data Protection Impact Assessment-'DPIA') ossia una Valutazione d'Impatto sulla protezione dei dati, in collaborazione con il RDP.
- ✓ La Valutazione d'Impatto deve contenere la descrizione dei trattamenti previsti e delle finalità, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità e una valutazione per i rischi per i diritti e le libertà degli interessati come le misure previste per affrontare i rischi.
- ✓ La Valutazione d'Impatto è richiesta in particolare nei seguenti casi:
 - ✓ Quando avviene una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la Profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono su dette persone fisiche;
 - ✓ Quando si effettua un trattamento su larga scala di dati sensibili e giudiziari;
 - ✓ Quando si effettua una sorveglianza sistematica su larga scala di una zona accessibile al pubblico
- ✓ ESCLUSIONI: il singolo professionista non ha necessità di nominare il DPO perché il trattamento non si considera «su larga scala», ma lo Studio con 20 Professionisti? Secondo le linee guida siamo in una zona «grigia»...



D.P.O.

Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (*Data Protection Officer* o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.



DPO/RPD (1/2)

Responsabile della Protezione dei Dati

Figura non contemplata nella attuale legislazione

- ✓ Il Titolare o il Responsabile del Trattamento dei Dati Personali devono designare un DPO ogni qualvolta:
 - ✓ il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico.
 - ✓ le attività principali del Titolare o del Responsabile consistano in trattamenti che, per loro natura, campo di applicazione e/o finalità richiedano il controllo regolare e sistematico degli interessati su larga scala;
 - ✓ il Titolare o il Responsabile trattino, su larga scala dati particolari (sensibili e/o giudiziari);
- ✓ L'RDP dovrà svolgere i suoi precisi compiti in autonomia e sarà dotato delle risorse necessarie per assolvere ai suoi compiti. Egli riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
- ✓ Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati.
- ✓ Può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Nei casi più complessi questa figura può essere rappresentata da un pool di esperti in materia.
- ✓ Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.



DPO/RPD (2/2)

Responsabile della Protezione dei Dati

- ✓ L'RDP deve essere designato in base alla sua comprovata professionalità e, in particolare, alla sua conoscenza specialistica della legislazione europea della protezione dei dati e della prassi in materia ed è tenuto, tra le altre cose a:
 - ✓ informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Nuovo Regolamento e da altre disposizioni dell'UE.
 - ✓ sorvegliare che il Nuovo Regolamento sia osservato;
 - ✓ fornire un parere in merito alla Valutazione d'Impatto (DPIA);
 - ✓ cooperare con l'autorità di controllo (Garante Privacy);
 - ✓ assicurare l'esercizio dei diritti degli interessati.
- ✓ L'RDP, per comprovare nel tempo al sua professionalità, dimostra di avere innanzitutto esperienza storica in materia e, successivamente, di aver effettuato dei corsi professionali e di aggiornamento periodici possibilmente certificati.
- ✓ ESCLUSIONI: il singolo professionista non ha necessità di nominare il DPO perché il trattamento non si considera «su larga scala», ma lo Studio con 20 Professionisti? Secondo le linee guida siamo in una zona «grigia»...



Il Responsabile del Trattamento (data processor agreement)

- ✓ Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
- ✓ I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
- ✓ Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento (previa autorizzazione scritta) per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto, gli stessi obblighi in materia di protezione dei dati contenuti nel tra il titolare del trattamento e il responsabile del trattamento.
- ✓ Il contratto o altro atto giuridico di cui ai paragrafi precedenti è stipulato in forma scritta, anche in formato elettronico.



Data breach e registro

(Violazione dei dati)

- ✓ Il Titolare e il Responsabile devono comunicare l'eventuale avvenuta Violazione di Dati Personali (Data Breach) entro 72 ore da quando ne vengono 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»*.
- ✓ Il Responsabile ha l'obbligo di informare il Titolare della eventuale violazione senza ingiustificato ritardo e quest'ultimo, a sua volta, deve notificare la violazione, senza ingiustificato ritardo, all'autorità Garante.
- ✓ È previsto, inoltre, un obbligo di comunicazione anche all'interessato, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- ✓ 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. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.
- ✓ Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
 - ✓ Eccezioni: crittografia, riduzione successiva rischio elevato, sforzo sproporzionato



Registri dei trattamenti (del Titolare e Responsabile)

- ✓ Il Titolare e il Responsabile del Trattamento devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente tutti gli specifici elementi di cui all'art. 30 del Nuovo Regolamento.
- ✓ L'obbligo di tenuta dei registri non si applica, in linea di principio, alle imprese o organizzazioni con meno di 250 dipendenti, a meno che si preveda il trattamento di dati sensibili e/o giudiziari, non sia occasionale o possa rappresentare un rischio per i diritti e le libertà dell'interessato.



Nuovi diritti dell'interessato

- ✓ Diritto all'oblio (art. 17). Evoluzione dell'attuale diritto alla cancellazione, il diritto del singolo interessato ad essere “dimenticato” dalle banche dati, dai mezzi di informazione, o dai motori di ricerca su base legislativa del Diritto all'Oblio.
 - ✓ Diritto di chiedere che siano cancellati i suoi dati personali che non siano più necessari per le finalità per le quali sono stati raccolti, da cui abbia ritirato il consenso al trattamento, si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme alla legge.
- ✓ Portabilità dei dati (art. 20) L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al Titolare, e di trasmettere i propri dati da un Titolare (ad esempio un social network) ad un altro Titolare (Data Portability), senza impedimenti da parte di colui al quale sono stati forniti in precedenza, qualora:
 - ✓ il trattamento si basi sul consenso
 - ✓ il trattamento sia effettuato con mezzi automatizzati

Avvocati e Garante...

✓ Aut. Gen. Garante 4/2016:

- ✓ Garanzie: «le autorizzazioni di carattere generale (...) sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati»
- ✓ Minimizzazione: «(...) i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati (...)». Es. dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità»
- ✓ Finalità: «(...) per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione»
- ✓ Informativa: «Resta inoltre fermo l'obbligo di informare l'interessato» (non per dati raccolti presso terzi)... come provarla?
- ✓ Conservazione: «(...) periodo strettamente necessario (...) I dati (...) non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene»
- ✓ Consenso: esclusioni: «il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali»
- ✓ Si applica anche l' Aut. Gen. Garante 2/2016...

Avvocati e GDPR...

- ✓ Misure tecniche adeguate al rischio:
 - ✓ Pseudonimizzazione
 - ✓ Crittografia
 - ✓ Autenticazione a due fattori
 - ✓ Back-up delocalizzato
 - ✓ Sistemi ridondati
 - ✓ Disaster recovery
 - ✓ Business continuity
 - ✓ Sistemi di monitoraggio della rete
 - ✓ Log AdS
 - ✓ MDM/MAM
 - ✓ Applicativi di data governance...
- ✓ Misure organizzative adeguate al rischio:
 - ✓ Manuale per l'uso degli strumenti informatici
 - ✓ Procedure (gestione utenze, assunzione e trattamento dati dei lavoratori, data breach, privacy by design e by default, etc.)
 - ✓ Tenuta registri
 - ✓ Controllo accessi
 - ✓ Formazione
 - ✓ Audit AdS e GDPR...



Grazie!

 BASSI DEL MORO
STUDIO LEGALE

Avv. Cesare C.M. Del Moro