pangea consulenze

CONVEGNO PRIVACY

Nuovo regolamento Europeo in materia di protezione die dati personali UE 679/16

Colle di Val d'Elsa, *20/04/18*

Relatore: Alessandro Corti
Responsabile Protezione dati (RPD)
Data Processor Officier (DPO)
Certificato secondo la norma UNI 11697:2017

LE NORMATIVE A CONFRONTO

D.Lgs.196 del 30 giugno 2003 *Codice in materia di protezione dei dati personali*	**Regolamento (UE) 2016/679 del 27 aprile 2016** *Relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*
Pubblicato in G.U. n.174 del 29 luglio 2003	Pubblicato in G.U.U.E. del 04 maggio 2016
Entrata in vigore: 01/01/2004	**Entrata in vigore:** 25/05/2016 ma si applica a decorrere dal 25/05/2018 (art.99)
Il D.Lgs.196/03 sarà abrogato dal 25/05/2018	*La Direttva 95/46/CE sarà abrogata a partire dal 25/05/2018 (Art.94 c.1)*

Le COLONNE del Regolamento UE

Responsabilizzazione
(Art.5 c.2)
Accountability

Principi base
(Art.5)

Principi di liceità del trattamento (Art.6)

Protezione fin dalla progettazione e per impostazione predefinita
(Art.25)
Privacy By design
Privacy By default

REGOLAMENTO UE 2016/679

Il concetto di «responsabilizzazione» o «accountability»

- Il Regolamento stabilisce una responsabilità globale del Titolare, denominata «**accountability**»
- Le nuove disposizioni «dettagliano l'obbligo di responsabilità del Titolare di rispettare il presente regolamento e di dimostrare tale conformità, anche mediante l'adozione di politiche interne e meccanismi per garantire tale rispetto»

Da **FORMA a SOSTANZA** mediante :

- l'attuazione del principio della protezione dei dati «by design» e «by default» (Art.25)
- Procedure interne (Art.32 c.4);
- la valutazione dei rischi (Art.32)
- la valutazioni di impatto sulla protezione dei dati, talvolta obbligatorie (art.35)
- Revisione periodica del sistema (Art.32 c.1 lett.d)

Le prescrizioni del Regolamento UE

Protezione dei dati fin dalla progettazione «by design»

Sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, quindi già in fase di progettazione, il Titolare, al fine di tutelare i diritti degli interessati ed essere conforme ai principi del GDPR, deve porre in essere «adeguate misure tecniche organizzative» (ad es. psudominizzazione, minimizzazione dei dati, misure di sicurezza ecc)

Protezione dei dati per impostazione predefinita «by default»

Secondo questo principio, devono essere adottati meccanismi che assicurino per impostazione predefinita:

- *siano utilizzati solo i dati necessari a uno scopo specifico (minimizzazione);*
- *i dati non siano resi accessibili ad un numero indefinito di persone (limitazione delle finalità);*
- *i dati non siano archiviati oltre il tempo necessario alla soddisfazione dello scopo (limitazione della conservazione);*

RACCOMANDAZIONI DEL GARANTE

MISURE DI SICUREZZA NEL TRATTAMENTO DEI DATI

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** *(si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento)*.
Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** *(si veda art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. **Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio** ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

PRINCIPI BASE

Reg.2016/679
Principi applicabili al Trattamento
Art.5 c.1

a) trattati in modo lecito e secondo correttezza e trasparenza nei confronti dell'interessato (liceità, correttezza e trasparenza);

- ***lecito:*** *deve basarsi su attività lecita e non illegale;*
- ***corretto****: deve essere chiaro e non ingannevole nei confronti dell'interessato;*
- ***trasparente:*** *per gli interessati dovrebbero essere trasparenti le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali che li riguardano. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*.

b) raccolti per finalità determinate, esplicite e legittime, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi (limitazione della finalità);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti o successivamente trattati (minimizzazione dei dati);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);

SANZIONI: € 20.000.000,00 o 4% del fatturato mondiale

PRINCIPI BASE

Reg.2016/679
Principi applicabili al Trattamento
Art.5 c.1

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (limitazione della conservazione);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza);

SANZIONI: € 20.000.000,00 o 4% del fatturato mondiale

LICEITA' DEI TRATTAMENTI

A condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato

SANZIONI: € 20.000.000,00 o 4% del fatturato mondiale

RACCOMANDAZIONI DEL GARANTE

LICEITA' DEL TRATTAMENTO
LEGITTIMO INTERESSE

Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **NON SPETTA** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di «responsabilizzazione» introdotto dal nuovo pacchetto protezione dati.

I - NOZIONI GENERALI

Reg.2016/679
Ambito di applicazione
Art.1

1.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**

SONO ESCLUSE LE IMPRESE INTENDENDO CON TALE TERMINE TUTTI I SOGGETTI CHE ESERCITANO ATTIVITA' ECONOMICA

Art.4 c.18 Regolamento UE:

la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

I - NOZIONI GENERALI

Reg.2016/679
Ambito di applicazione
Art.2

1.Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali **contenuti in un archivio o destinati a figurarvi**.

ARCHIVIO (Art.4 c.6)
qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

I - NOZIONI GENERALI

Reg.2016/679
Ambito di applicazione TERRITORIALE
Art.3

1.Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno **stabilimento*** da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, *indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*

2.Il presente regolamento si applica al **trattamento dei dati personali di interessati che si trovano nell'Unione**, effettuato da un titolare del trattamento o da un responsabile del trattamento **che non è stabilito nell'Unione**, quando le attività di trattamento riguardano:

a)l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b)il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione

3.Il presente regolamento si applica al trattamento dei dati personali effettuato da un **titolare del trattamento che non è stabilito nell'Unione**, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

***STABILIMENTO (Art.4 c.16)**
il luogo della sua amministrazione centrale nell'Unione da cui vengono prese le decisioni sulle finalità e i mezzi del trattamento di dati personali

I - NOZIONI GENERALI

ESCLUSIONI DAL CAMPO DI APPLICAZIONE

Art.2 c.2.

- Trattamento effettuato al di fuori delle CE
- Trattamenti effettuati da persona fisica per l'esercizio di attività a **carattere esclusivamente personale o domestico**;
- Effettuato da autorità competenti a fini di prevenzione, indagine ecc

GLI STEP PER L'ADEGUAMENTO

Step 1

Censimento dei trattamenti

- *Definizione gli ambiti di trattamento per funzioni o processi*
- *Classificazione dei dati*
- *Rilevazione dei flussi dei dati interni/esterni*

Step 2

Definire ruoli e responsabilità

- *Individuare il titolare del trattamento*
- *Individuare i Responsabili del trattamento*
- *Individuare tutti gli incaricati del trattamento*
- *Individuare gli amministratori di sistema*
- *Nomina Responsabile Trattamento Dati*

Step 3

Verifica degli adempimenti:

- *Modelli di informative per gli interessati*
- *Modelli di consenso*
- *Lettere agli incaricati*
- *Registro dei trattamenti*
- *Contratti per i Responsabili e/o contitolari*
- *Valutazione di impatto*
- *Contratti o altra documentazione per l'esportazione dei dati*

GLI STEP PER L'ADEGUAMENTO

Step 4

Misure di sicurezza

- *Valutazione dei rischi*
- *Verifica delle misure di sicurezza adottate:*
  - *Minime*
  - *Adeguate*

Step 5

Formazione

- *Incaricati al trattamento*

Step 6

Audit

- *Audit di mantenimento*

Step 7

Aree specifiche

- *Videosorveglianza*
- *Siti Web*
- *Profilazione*
- *Monitoraggio clienti/utenti*
- *RFID*

pangea consulenze

STEP 1

CENSIMENTO DEI TRATTAMENTI

CONCETTO DI DATO PERSONALE

D.Lgs.196/03 **Dato Personale** *Art.4 c.1 lett.b*	Reg.2016/679 **Dato Personale** *Art.4 c.1*
Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione*, **identificati o identificabili, anche indirettamente**, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale * Lettera così modificata dall'art. 40, comma 2, lett. a), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214	Qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»). *Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con:* - *particolare riferimento a un identificativo come il nome,* - *un numero di identificazione,* - *dati relativi all'ubicazione,* - *un identificativo online o* - *a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*

CONCETTO DI DATO PERSONALE

decisione Garante

il Garante ha precisato che l'espressione **qualunque informazione** vuole attribuire alla definizione di *dato personale* la massima ampiezza, comprendendo anche ogni notizia, informazione o elemento che abbia un'efficacia informativa tale, da fornire un contributo aggiuntivo di conoscenza rispetto ad un soggetto identificato od identificabile

CONCETTO DI DATO PERSONALE

Sono ad esempio dati personali:

- gli indirizzi, i recapiti, i numeri di telefono
- i suoni come le registrazione di conversazioni
- le immagini (es. video-sorveglianza)
- dati biometrici (impronte digitali, dell'iride ecc)
- dati genetici
- Le valutazioni di carattere soggettivo come ad esempio:
  - le valutazioni, effettuate da una banca, sul grado di affidabilità di un soggetto che richiede un finanziamento, nonché le eventuali motivazioni anche "interne" che sono alla base del rifiuto di concederlo
  - una diagnosi medica, anche per la parte che comprende elementi valutativi o di prognosi di tipo discrezionale
  - le note di qualifica, cioè le valutazioni che contribuiscono a formare il giudizio annuale sul rendimento di un dipendente

CLASSIFICAZIONE DEI DATI

NATURA DEL DATO

- Comune
- Particolare *(ex Sensibile)* e/o giudiziario (art.9 e 10)

TIPOLOGIA DATO

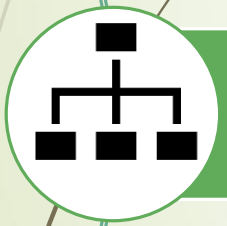
- Cartaceo
- Elettronica

STEP 1 – CENSIMENTO DEI TRATTAMENTI

INDIVIDUARE TUTTI I FLUSSI DI TRATTAMENTO

INPUT
- Dati

- Dati forniti direttamente dall'interessato o da terzi
- Videosorveglianza
- Geolocalizzazione, web .....



TRATTAMENTI
- Interni
- Esterni

- Incaricati interni e Responsabili esterni
- Profili di accesso
- Procedure di trattamento

OUTPUT
- Comunicazione
- Utilizzo

- Uso dei dati in funzione delle finalità che possono prevedere comunicazione a terzi, archiviazione, ecc

Trasparenza

pangea consulenze

STEP 2

DEFINIZIONE DI RUOLI E RESPONSABILITA’

STEP 2 – DEFINIZIONE DI RUOLI E RESPONSABILITA'

FILIERA DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO
Data Processor (DP)
(solo esterno)

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)
Data Protection Officier (DPO)

~~**INCARICATO**~~ **ADDETTO AL TRATTAMENTO**

pangea consulenze

STEP 4

VALUTAZIONE DEI RISCHI

STEP 4 – Valutazione dei rischi

MISURE DI SICUREZZA DA ADOTTARE

Misure minime di sicurezza

Disciplinare Tecnico-Allegato B
D.Lgs.196/03

Misure idonee di sicurezza

Art.31 D.Lgs.196/03

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione ***di idonee e preventive misure di sicurezza****, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

(TUTELA DA ART.2050 CC)

NOVI

pangea consulenze

STEP 4 – Valutazione dei rischi

SICUREZZA DEI DATI PERSONALI
da Art.32 a art.34

Art.32 c.1 – Sicurezza del trattamento

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

- *la pseudonimizzazione e la cifratura dei dati personali;*
- *la capacità di assicurare su base permanente 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.*

SANZIONI: € 10.000.000,00 o 2% del fatturato mondiale

pangea consulenze

STEP 5

FORMAZIONE

NOVI TA'

pangea consulenze

STEP 5 – Formazione

Art.32 c.4
Il titolare del trattamento e il responsabile del trattamento **fanno sì** che chiunque agisca sotto la loro autorità e abbia accesso a dati personali **non tratti tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

FORMAZIONE OBBLIGATORIA DI TUTTA LA FILIERA DEL TRATTAMENTO
REALE

SANZIONI: € 10.000.000,00 o 2% del fatturato mondiale

pangea consulenze

STEP 6

AUDIT

STEP 6 – AUDIT

Il regolamento prevede la necessità di una verifica periodica del sistema privacy in particolare:

- Art.32 c.1 lett.d (Sicurezza del trattamento)

  Il titolare mette in atto una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche organizzative al fine di garantire la sicurezza del trattamento;

- Art.39 c.1 lett.b

  Il Dpo ha l'obbligo di sorvegliare sull'osservanza del presente regolamento nonché delle politiche adottate dal titolare….

pangea
consulenze

SANZIONI

SANZIONI

Art.83 c.4 – Sanzioni amministrative pecuniarie **fino a € 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per la violazione inerente la mancata:

- *designazione dei responsabili*
- *desiganzione del Responsabile della sicurezza dei dati*
- *documentazione relativa a ciascun trattamento di dati personali*
- *sicurezza del trattamento*
- *notifica delle violazioni dei dati*
- *comunicazione delle violazioni agli interessati*
- *Privacy by design e privacy by default*
- *cooperazione con l'autorità di vigilanza*
- *valutazione di impatto sulla protezione dei dati*
- *…….*

SANZIONI

Art.83 c.4 – Sanzioni amministrative pecuniarie **fino a € 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per la violazione inerente la mancata:

- *designazione dei responsabili*
- *desiganzione del Responsabile della sicurezza dei dati*
- *documentazione relativa a ciascun trattamento di dati personali*
- *sicurezza del trattamento*
- *notifica delle violazioni dei dati*
- *comunicazione delle violazioni agli interessati*
- *Privacy by design e privacy by default*
- *cooperazione con l'autorità di vigilanza*
- *valutazione di impatto sulla protezione dei dati*
- *…….*

SANZIONI

Art.83 c.4 – Sanzioni amministrative pecuniarie **fino a € 20.000.000,00, o per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per la violazione inerente:

- *trattamento dei dati senza rispettare i principi di: liceità, correttezza,trasparenza, limitazione delle finalità, minimizzazine dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.*
- *trattamento dei dati in assenza del consenso o acquisito non in modo corretto;*
- *Trattamento dei dati in assenza di una delle condizioni che lo rendono lecito anche senza il consenso (Art.6)*
- *Trattamento di dati di minori senza il consenso se necessario;*
- *Trattamento illecito di particolari categorie di dati (ex sensibili)*
- *Violazione dei diritti dell'interessato: accesso, oblio, rettifica, limitazione del trattamento, portabilità dei dati;*
- *Mancata informativa del trattamento dei dati*
- *Violazione delle regole di trattamento mediante profilazione o processi decisionali automatizzati relativo a persone fisiche;*
- *Trasferimento illecito di dati personali all'estero*

SANZIONI

Art.84 – Gli stati membri possono stabilire norme relative all'applicazione di altre sanzioni per la violazione del regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma del presente regolamento (Art.83).

COSA DA FARE OGGI FINO AL 24 MAGGIO 2018…

1. Fare nuovo censimento di tutti i dati e dei trattamenti: *individuare i dati trattati, individuare la base giuridica, verificare la durata della conservazione dei dati e a chi vengono comunicati…*
2. Trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche: *verificare se via siano trattamenti di questo tipo e in caso affermativo effettuare la valutazione di impatto sulla privacy (PIA – Privacy Impact Assessment)*
3. Formalizzare organigramma della privacy: *identificare le varie figure coinvolte nel trattamento (sia interni che esterni), verificare che gli incarichi ai Responsabili siano contrattualizzati, verificare che i Responsabili esterni non abbiano dei sub-responsabili, individuare gli incaricati al trattamento, verificare che non ci si trovi nella situazione di Contitolarità (es. studi associati)*
4. Nominare il Responsabile della Protezione dei dati *ove obbligatorio o opportuno*
5. Redigere il registro dei trattamenti
6. Formare tutto il personale

GRAZIE
PER L'ATTENZIONE !!!!!

Potete inviare domande o richieste alla seguente email: a.corti@pangeaconsulenze.it