consolve
Consulting & Solutions, not else.

CONFINDUSTRIA FIRENZE

IL NUOVO REGOLAMENTO UE (679/2016) SULLA PRIVACY

COSA CAMBIA PER LE AZIENDE?

Avv. Marco Giuri

marcogiuri@studiogiuri.it

www.studiogiuri.it

Tutela della Privacy
Introduzione alla disciplina

- Riservatezza come diritto pluri-funzionale:
- potere di interrompere il flusso di informazioni
- potere di "seguito"
- potere di controllo nel modo di utilizzo
- tutela di dignità e uguaglianza nei dati sensibili
- DIRITTO PROTEZIONE DATI PERSONALI

FONTI NORMATIVE

- DIRETTIVA 95/46/CE: abrogata!
- CODICE PRIVACY
- LINEE GUIDA GARANTE PRIVACY
- PROVVEDIMENTI GARANTE
- CODICE CIVILE
- CODICE PENALE
-

Diritto della Protezione dei dati - Regolamento

Anche il Regolamento prevede la privacy delle ***persone fisiche*** come un **DIRITTO FONDAMENTALE** cosi come era previsto dalla Direttiva 95/46/EU

Il Trattamento dei dati personali deve essere a servizio dell'uomo.

Il diritto alla protezione dei dati personali NON è una prerogativa assoluta ma va contemperato con altri diritti fondamentali (principio del pari grado)

Obiettivi del Regolamento

Garantire la certezza del diritto

La Trasparenza agli operatori economici

Garantire a tutti i cittadini UE gli stessi diritti

Definire stessi obblighi e responsabilità dei Titolari / Responsabili del trattamento

Stabilire sanzioni uguali in tutti i Paesi EU

Cooperazione fra Autorità di controllo

Regolamento EUROPEO

Regolamento UE 679/2016

Entrerà in vigore il **25 maggio 2018**

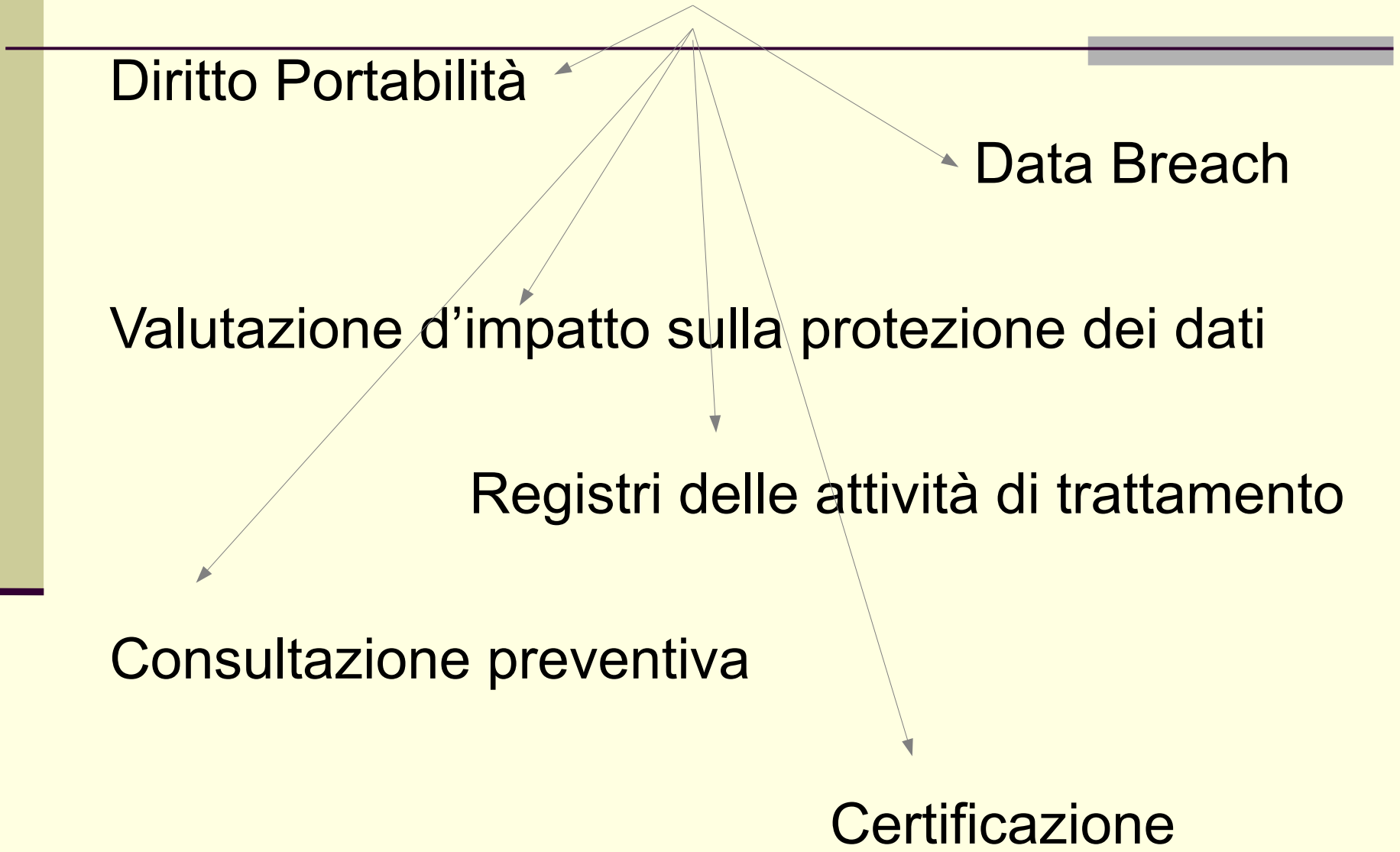
Perché Nuovo Regolamento?

a)Continua evoluzione dei concetti di privacy e protezione dati

b)Diffusione del progresso tecnologico

c)Massima diffusione di dati: condivisione dei dati ai massimi livelli

ALCUNE NOVITA' RILEVANTI



Data Breach - Articolo 33

Novità rilevante

In caso di violazione dei dati personali, il Titolare del trattamento **notifica** la violazione **all'autorità di controllo competente** senza ingiustificato ritardo, ove possibile **entro 72 ore dal momento della conoscenza**, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

Se non viene effettuata entro 72 ore, la notifica è corredata di una giustificazione motivata

Contenuto Minimo Notifica Data Breach

a)DESCRIZIONE natura della violazione, le categorie violate, il numero di interessati

b)Il nome e le coordinate di contatto del DPO

c)Descrivere le probabili conseguenze della violazione

d)Descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione

Obbligo Responsabile Trattamento

Il Titolare **documenta** qualsiasi violazione dei dati personali incluse le circostanze in cui si è verificata, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.

ACCOUNTABILITY

Comunicazione all'interessato

Comunicazione di una violazione all'interessato: quando la violazione dei dati è suscettibile di presentare un rischio elevato per i diritti delle persone, il titolare del trattamento comunica la violazione all'interessato **SENZA INGIUSTIFICATO RITARDO. Va usato linguaggio semplice e chiaro per spiegare la violazione.**

Comunicazione all'interessato

Non è richiesta la comunicazione se:

1)Il titolare aveva utilizzato le misure tecniche ed organizzative adeguate alla protezione e tali misure hanno difeso i dati oggetto di violazione: es. cifratura - OPPURE

2)Il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti degli interessati, O

3)Detta comunicazione comporterebbe sforzi sproporzionati: **si fa comunicazione pubblica**

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Articolo 35: La fa il **Titolare del Trattamento.**

Regola generale

Quando? (Prima di procedere al trattamento)

Quando un tipo di trattamento, allorchè prevede uso di nuove tecnologie, considerati la natura, il campo di applicazione, il contesto e le finalità del trattamento **può presentare un RISCHIO ELEVATO per i diritti e le libertà delle persone. Chiede un parere a DPO.**

Casi specifici di Valutazione d'Impatto

Regola specifica

Va fatta la valutazione d'impatto **in questi casi**:

a)Una valutazione SISTEMATICA E GLOBALE di aspetti personali relativi a persone fisiche, basata su trattamento automatizzato, compresa profilazione,

b)Il trattamento su **larga scala** di dati sensibili o dati giudiziari

c)La sorveglianza sistematica di una zona accessibile al pubblico su larga scala

Autorità e Valutazione d'Impatto

Autorità di controllo **redige e pubblica** un elenco di tipologie di trattamenti soggetti al requisito di una valutazione d'impatto.

Autorità di controllo può anche redigere e pubblicare un elenco delle tipologie di trattamenti che non sono soggetti a valutazione d'impatto.

MECCANISMO DI COERENZA: prima di adottare tali elenchi, l'Autorità applica il meccanismo di coerenza: richiede un'operazione di controllo delle Autorità per un'applicazione coerente del Regolamento

Contenuto **Minimo** Valutazione Impatto

a)Descrizione sintetica dei trattamenti e delle finalità e l'interesse legittimo perseguito dal responsabile del trattamento

b)Una valutazione della necessità e proporzionalità dei trattamenti rispetto alle finalità

c)Una valutazione dei rischi per i diritti degli interessati

d)Le misure previste contro questi rischi

Autorità di Controllo: POTERI

Art. 58 POTERI

Poteri di indagine, poteri correttivi: es avvertimenti al titolare - Responsabile su possibili violazioni

Rivolgere moniti se ci sono state violazioni.

Ingiungere al titolare-responsabile del trattamento o all'incaricato di soddisfare le richieste dell'interessato di esercitare i suoi diritti

Ingiungere al titolare - Responsabile o incaricato di conformare i trattamenti al Regolamento

Imporre limitazioni provvisorie al trattamento

Autorità di Controllo: POTERI

POTERI CORRETTIVI

POTERI AUTORIZZATIVI E CONSULTIVI

Autorità di Controllo: POTERI

POTERI CORRETTIVI

Avvertimenti che ci potrebbero essere possibili violazioni

Moniti dove ci sono violazioni

Ingiunzioni: soddisfare diritti interessato / conformare i trattamenti al Regolamento /comunicare all'interessato una violazione

Imporre una limitazione provvisoria

Ordinare la rettifica, limitazione e cancellazione

Ritirare la certificazione

Irrogare una sanzione pecuniaria e misure correttive

Ordinare la sospensione di flussi dati vs. Paesi Terzi

Autorità di Controllo: POTERI

POTERI AUTORIZZATIVI E CONSULTIVI

1) Consulenza al titolare - Responsabile: procedura consultazione preventiva
2) formulare pareri a Parlamento / Governo / PA
3) autorizzare il trattamento per Paesi terzi
4) accreditare gli organismi di certificazione
5) rilasciare certificazioni
6) autorizzare la clausole contrattuali

Altri poteri fissati da legge nazionale.

Comitato Europeo per la Protezione Dati

Organismo dell'Unione: il rappresentante per ogni Stato è al suo interno + Garante EU

Compiti <u>innumerevoli (24 compiti)</u>

a)Monitora e assicura piena applicazione del Regolamento

b)Fa proposte di modifica del Regolamento

c)Pubblica linee guida, raccomandazioni, best practice

d)Incoraggia Codici di Condotta

e)Effettua accreditamento Organismi di Certificazione

MISURE DI SICUREZZA
Regolamento

Articolo 32: TITOLARE E RESPONSABILE mettono in atto MISURE TECNICHE ED ORGANIZZATIVE adeguate per garantire (e riuscire a dimostrare) che il trattamento è conforme al Regolamento.

Si tiene conto di: stato dell'arte/costi attuazione/natura/campo di applicazione/contesto/finalità del trattamento/ rischio e probabilità per i diritti e le libertà dei soggetti persone fisiche

MISURE DI SICUREZZA
Regolamento

Articolo 32

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:*

Misure di sicurezza

Titolare/Responsabile sceglie le misure tecniche ed organizzative adeguate per GARANTIRE un l**ivello di sicurezza ADEGUATO** al rischio e comprendono, tra l'altro:

-Cifratura e pseudonimizzazione

-Capacità di assicurare la continua riservatezza, integrità, disponibilità dei sistemi

-Capacità di ripristino tempestivo dei dati in caso di incidente fisico o tecnico

-Una procedura per provare/verificare/ valutare l'efficacia delle misure scelte

Misure di sicurezza

Per Valutare l'adeguato livello di sicurezza tengo conto di:

- rischio distruzione
- rischio perdita
- rischio modifica
- rischio divulgazione non autorizzata
- rischio accesso illegale

N.B.: L'applicazione di un CODICE DI CONDOTTA o di una CERTIFICAZIONE può essere utilizzata come **elemento per dimostrare la conformità** ai requisiti delle misure di sicurezza

Chi tratta i dati deve essere ISTRUITO dal responsabile sulle misure di sicurezza

RISARCIMENTO DANNO

stessi principi Direttiva 46/95

art 82 Chiunque subisca un danno materiale o immateriale cagionato da una violazione del Regolamento ha il diritto di ottenere il **risarcimento del danno** dal titolare o responsabile

SANZIONI REGOLAMENTO

Articolo 83-84

Le sanzioni sono diventate pesanti rispetto alla precedente normativa.

Le sanzioni vengono irrogate dalle Autorità di Controllo che devono rispettare i principi di

EFFETTIVITA'

PROPORZIONALITA'

DISSUASIVITA'

Sanzioni

Quando si deve irrogare una sanzioni amministrativa e si deve fissare l'ammontare si deve tener conto, caso per caso, di:

a)NATURA, GRAVITA' E DURATA DELLA VIOLAZIONE in considerazione della natura, del campo di applicazione o delle finalità del trattamento nonché il numero degli interessati lesi dal danno e del livello di danno subito

b)Carattere doloso o colposo della violazione

c)Misure prese dal titolare/responsabile per ATTENUARE il danno subito da interessati

Sanzioni

d) Il grado di responsabilità del titolare e del responsabile considerate le misure tecniche e organizzative messe in atto

e) Precedenti violazioni pertinenti

f) Grado di cooperazione con Autorità per porre rimedio alla violazione e attenuare effetti negativi

g) Categorie di dati interessati dalla violazione

h) Se c'è stata notificazione o meno della violazione

i)Se ci siano stati precedenti provvedimenti nei confronti del responsabile e se li abbia rispettati

l) Adesione a codici di condotta o a meccanismi di certificazione

m) Fattori aggravanti o attenuanti applicabili al caso: vantaggi finanziari, perdite evitate.

MISURA DELLA SANZIONE

LIMITE IN CASO DI PIU' VIOLAZIONI

Se in relazione allo stesso trattamento o a trattamenti collegati il titolare/responsabile VIOLA (con dolo o colpa) varie disposizioni del Regolamento, l'importo totale delle sanzioni amministrativa pecuniaria NON può superare l'importo precisato per la violazione più grave.

Misura delle sanzioni

La violazione di determinate norme è soggetta a sanzioni fino a **20.000.000 di Euro o, per le Imprese, fino al 4% del fatturato mondiale** annuo dell'esercizio precedente se superiore.

-PRINCIPI DI BASE DEL TRATTAMENTO E CONSENSO

-Diritti degli interessati

-I trasferimenti di dati all'estero

-Mancata osservanza di un ordine, limitazione o sospensione trattamento da Autorità di controllo

Misura delle sanzioni

Altre sanzioni sono **fino a 10.000.000, o per le imprese, fino al 2% del fatturato mondiale** annuo dell'esercizio precedente se superiore:

a)Obblighi del titolare e del responsabile

b)Obblighi dell'organismo di certificazione

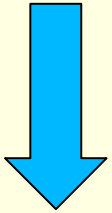
c)Obblighi dell'organismo di controllo

Misura sanzioni

La mancata osservanza di un **ordine da parte dell'autorità di controllo** soggetta a sanzioni amministrative pecuniarie fino a 20.000.000, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Discrezionalità Paesi

Conferisce una certa discrezionalità agli Stati membri



Gli Stati membri determinano le sanzioni per le violazioni del Regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie.