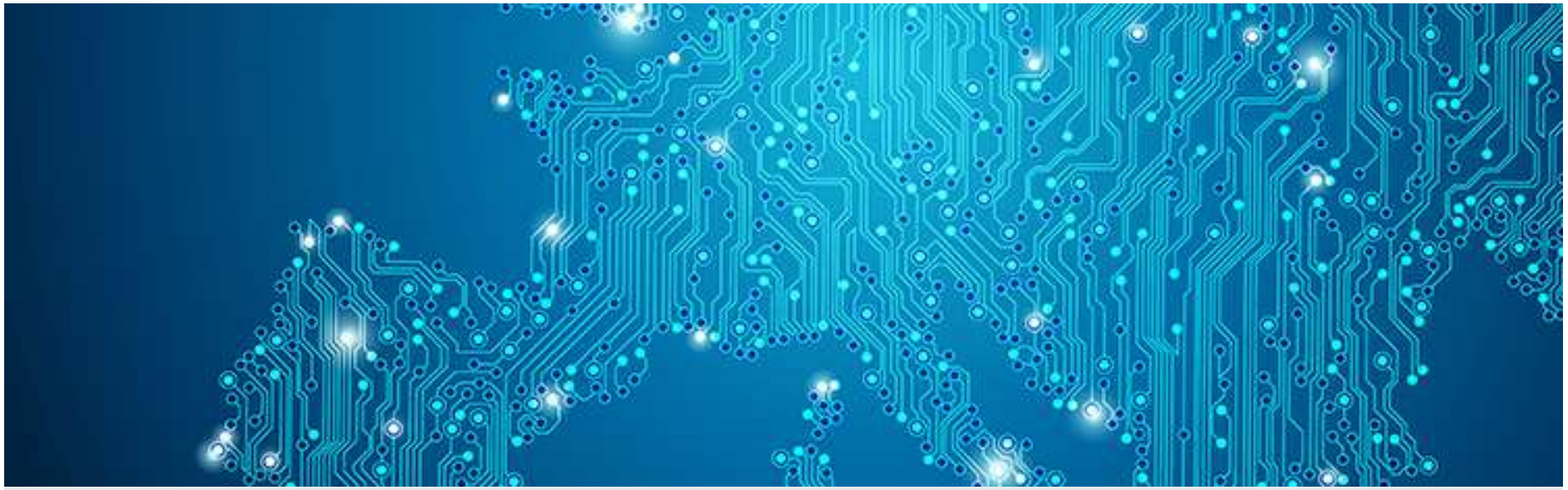
DNV·GL



BUSINESS ASSURANCE

General Data Protection Regulation

Tempo di agire.

20 March 2018

Commercial in confidence

CHE COS'E' IL GENERAL DATA PROTECTION REGULATION?

- Dopo **4 anni** di preparazione e dibattito è stato approvato il **GDPR** dal Parlamento Europeo il **27 aprile 2016**.
- Come prevede l'art. 99 il Regolamento si applicherà a decorrere dal **25 maggio 2018**
- Il nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali n. 2016/679 (GDPR), con i suoi 99 articoli ha **riscritto la disciplina della Privacy a livello europeo.**
- La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla **continua evoluzione** degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente **alla diffusione del progresso tecnologico.**
- Quando si parla di privacy parliamo di dati relativi alle Persone Fisiche

IL QUADRO NORMATIVO APPLICABILE IN ITALIA

Regolamento 2016/679	**IN VIGORE,** pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	**IN VIGORE,** decade il 24 maggio 2018
Codice D.Lgs. 196/2003	**VIGORE, NON DECADE**, dovrà essere coordinato con il reg. UE secondo i criteri indicati dalla Legge di Delegazione
Provvedimenti Autorità Garante	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Accordi Internazionali su Trasferimento dati	**VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissioni UE	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificate, sostituite, abrogate

OBIETTIVI ED IMPLICAZIONI DEL GDPR PER LE ORGANIZZAZIONI

Obiettivi

Definire una BASELINE per la protezione dei dati

Proteggere e tutelare meglioo la protezione dei dati di tutti I cittadini in Europa

Armonizzare la normativa in Europa in materia Privacy eliminando le differenze di approccio tra Stati membri

Implicazioni

Sanzioni fino a €20,000,000 o al 4% del fatturato (tra I due valori verrà scelto quello più gravoso)

Rischio Reputazionale

Incrementare il potere degli individui qualora si verificasse una violazione dei dati personali

OGGETTO E FINALITA'

Definire una BASELINE per la protezione dei dati

Proteggere e tutelare meglio la protezione dei dati di tutti I cittadini in Europa

Armonizzare la normativa in Europa in materia Privacy eliminando le differenze di approccio tra Stati membri

One continent, one law: a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28. The benefits are estimated at €2.3 billion per year.
Fonte: Ufficio Stampa Commissione Europea http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

Il Regolamento si applica:

1. alla protezione delle **persone fisiche** con riguardo al trattamento dei loro **dati personali**
2. al **trattamento automatizzato** di dati personali
3. al **trattamento NON automatizzato** di dati personali contenuti in un **archivio**

COSA SI INTENDE PER DATO PERSONALE

Ai fini del regolamento per "**dato personale**" si intende 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**.

Art. 4 - Definizioni

196/2003	GDPR
"**dato personale**", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale	«**dato personale**»: 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

Art. 4 - Definizioni

196/2003	GDPR
"**dati sensibili**", i 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, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;	È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il GDPR

Cos'è il **trattamento** di un dato?
Qualsiasi attività di gestione del dato come:

- ✓ la raccolta,
- ✓ la conservazione,
- ✓ la modifica,
- ✓ la consultazione,
- ✓ la comunicazione,
- ✓ la cancellazione

su qualsiasi supporto

- ✓ informatico,
- ✓ cartaceo o analogico,

sia attraverso operatori sia con processi automatizzati

Art. 4 - Definizioni

196/2003	GDPR
"**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 di dati;	«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Art. 4 - Definizioni

196/2003	GDPR
"**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31	Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). **Principio di Accountability**

Art. 4 - Definizioni

196/2003	GDPR
Art. 33. Misure minime 1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.	Protezione dei dati fin dalla progettazione (by design) e protezione per impostazione predefinita (by default) …il titolare del trattamento mette in atto misure tecniche e organizzative adeguate… …per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento… (Principio di minimizzazione)

Art. 4 - Definizioni

196/2003	GDPR
	«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

BUSINESS ASSURANCE

I 7 PRINCIPI DEL GDPR

20 March 2018

Commercial in confidence

GDPR – I 7 PRINCIPI

I 6 elementi di leicità del trattamento (40-44)

Consenso: l'interessato ha dato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;

Esecuzione contrattuale: l'elaborazione è necessaria per l'esecuzione di un contratto a cui l'interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto;

Obbligo legale: l'elaborazione è necessaria per adempiere a un obbligo legale a cui è soggetto il responsabile del trattamento;

Interesse vitale delle persone: il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica;

Interesse pubblico: il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento;

Interesse legittimo: il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte

PRINCIPIO DI CORRETTEZZA

La correttezza del trattamento è essenzialmente legata all'idea che gli interessati devono essere **consapevoli** del fatto che i loro dati personali saranno trattati, compreso il modo in cui i dati saranno raccolti, conservati e utilizzati, per consentire loro di **prendere una decisione informata**

PRINCIPIO DI TRASPARENZA

- Il **principio della trasparenza** impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Principio di Trasparenza

- Il principio di Trasparenza non è direttamente spiegato nel GDPR, se ne fa maggiore chiarezza nell'Art. 12

> Art. 12
>
> "…in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Principio di Trasparenza

"**conciso e trasparente**" i Titolari dovrebbero presentare le informazioni/comunicazioni (1) in modo efficiente e succintamente al fine di (2) evitare l'affaticamento delle informazioni. Queste informazioni dovrebbero essere (3) chiaramente differenziate da altre informazioni non relative alla privacy, come le disposizioni contrattuali.

(4) In un contesto online, l'uso di una dichiarazione / informativa sulla privacy a più livelli consentirà a un soggetto dei dati di navigare verso la particolare sezione della dichiarazione / informativa sulla privacy a cui desiderano accedere immediatamente, piuttosto che dover scorrere grandi quantità di testo alla ricerca di particolari problemi.

"**intelligibile**" significa che (1) dovrebbe essere compreso da un membro medio del pubblico previsto. Ciò significa che il Titolare deve prima identificare il pubblico previsto e accertare il livello medio di comprensione del membro. Poiché il pubblico previsto può, tuttavia, differire dal pubblico effettivo, il Titolare dovrebbe anche (2) controllare regolarmente se le informazioni / comunicazioni sono ancora adattate al pubblico reale (in particolare dove comprende minori), e apportare modifiche se necessario. I Titolari possono dimostrare la loro conformità con il principio di trasparenza (3) testando l'intelligibilità delle informazioni e l'efficacia delle interfacce / comunicazioni / politiche utente ecc., attraverso i pannelli utente.

Commercial in confidence

Principio di Trasparenza

Consequence: Una considerazione centrale del principio di trasparenza delinea che l'interessato dovrebbe essere in grado di (1) determinare in anticipo quale sia l'ambito e le conseguenze del trattamento. Il WP29 ritiene che i Titolari non dovrebbero solo fornire le informazioni prescritte ai sensi degli articoli 13 e 14, ma anche pronunciare separatamente in (2) un linguaggio non ambiguo quali sono le conseguenze più importanti del l'elaborazione (3) non basandosi su esempi di elaborazione dei dati "innocenti" e prevedibili, ma fornendo una panoramica dei tipi di trattamento che potrebbero avere il maggiore impatto sui diritti e le libertà fondamentali dei dati soggetti in relazione alla protezione dei propri dati personali.

"**facilmente accessibile**" significa che l'interessato non deve cercare le informazioni e che dovrebbero essere (1) immediatamente evidente a loro dove è possibile accedere a queste informazioni, ad esempio fornendole direttamente a loro, collegandole ad esse, segnalandole chiaramente o come risposta a una domanda di lingua naturale (ad esempio in una privacy online a più livelli), dichiarazione / avviso, FAQ, tramite popup contestuali che si attivano quando un soggetto di dati compila un modulo online o in un contesto digitale interattivo attraverso un'interfaccia chatbot, ecc.).

Principio di Trasparenza

"**Linguaggio chiaro e semplice**" devono essere seguite le migliori (1) pratiche per una scrittura chiara. Il richiamo al linguaggio chiaro è presente anche nel Considerando 42. Le informazioni dovrebbero essere fornite nel modo più semplice possibile, evitando complesse perifrasi. L'informazione dovrebbe essere (2) concreta e definitiva; (3) non dovrebbe essere formulato in termini astratti o ambivalenti o lasciare spazio a interpretazioni diverse.

Vedi: How to Write Clearly by the European Commission (2011) https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5

"**in particolare nel caso di informazioni destinate specificamente ai minori**". Se un Titolare si rivolge ai minori o se è consapevole del fatto che la sua offerta è utilizzata dai minori (facendo affidamento sul consenso del minore- over 16), (1) dovrebbe utilizzare un vocabolario, un tono e uno stile appropriato per un sedicenne.

Un utile esempio di linguaggio centrato sul bambino usato come alternativa alla lingua legale può essere trovato nella "Convenzione delle Nazioni Unite sui diritti dell'infanzia".

https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

PRINCIPIO DI LIMITAZIONE DELLE FINALITA'

- I Titolari devono innanzitutto identificare le particolari finalità per le quali i dati personali saranno trattati (by design)
- Tali scopi diverranno i limiti entro i quali i dati personali devono essere raccolti e utilizzati dai responsabili del trattamento dei dati.
- Il trattamento secondario può essere effettuato legalmente solo quando tale trattamento è considerato compatibile con lo scopo originale per il quale i dati personali sono stati raccolti.

I principi: limitazione delle finalità

Esempio 1

- I Titolari raccolgono ed elaborano i dati personali per offrire servizi legati a **un'applicazione mobile di fitness**.
- Lo scopo del trattamento dei dati è analizzare i dati per raccomandare all'utente una routine di allenamento personalizzata.
- Un ulteriore elaborazione dei dati per identificare errori tecnici dell'applicazione sarà considerata compatibile, poiché migliorare l'efficienza dell'app è in linea con lo scopo originale.

Fonte: IAPP_E_TB European Data Protection "6.2.3, p. 271

Esempio 2

- Per assistere i **pazienti diabetici nell'erogazione di farmaci**, viene sviluppata un'app che offre il monitoraggio dei livelli di concentrazione di zucchero nel sangue.
- L'app condivide le informazioni personali con un'azienda che vende farmaci per il diabete. La promozione e la commercializzazione dei farmaci per il diabete non sono compatibili con lo scopo originale.
- "Code of Conduct on privacy for mobile health applications" pubblicato il 7 Giugno 2016. https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

Esempio 3

- Un **professionista della salute raccoglie dati personali** per essere in grado di valutare e trattare le condizioni mediche dei suoi pazienti.
- La condivisione dell'elenco dei pazienti con una compagnia assicurativa per consentire alla compagnia assicurativa di offrire i propri servizi (ad es. Assicurazione sulla vita o sanitaria) non sono compatibili con lo scopo originale per il quale i dati personali sono stati raccolti.

PRINCIPIO DI MINIMIZZAZIONE DEI DATI

- Il principio della "minimizzazione dei dati" indica che un Titolare del trattamento dei dati dovrebbe limitare la raccolta di informazioni personali a ciò che è **direttamente rilevante e necessario per raggiungere uno scopo specifico**.

- Dovrebbero inoltre conservare i dati **solo per il tempo necessario** a raggiungere lo scopo.

PRINCIPIO DI ESATTEZZA

- I dati raccolti dovranno essere esatti e, se necessario, aggiornati.
- Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

Esatezza

- Se un individuo si è trasferito da Chester a Wilmslow, un record che mostra che attualmente vive a Chester è ovviamente impreciso. Se l'archivio rappresenta lo storico abitativo invece è esatto. Deve sempre essere chiaro cosa è destinato a mostrare l'archivio.
- Un giornalista include informazioni derivate da Internet sull'arresto per guida pericolosa. Se il giornalista riporta "la fonte non è stata verificata" il dato è esatto. Se non lo fa, lasciando intendere al pubblico che l'informazione è verificata, il dato è inesatto.
- Il Postcode Address File contiene gli indirizzi postali delle abitazioni nel Regno Unito. Riflette la consegna la posta della Royal Mail. Capita che un indirizzo postale sia collegato a una città in una contea (ad es. Stoke-on-Trent nello Staffordshire) anche se l'ubicazione reale è in un'altra contea (ad es. Cheshire). Il file PAF è esatto per la sua funzione (consegna posta).
- "è accettabile tenere registri di eventi accaduti per errore, a condizione che tali registri non siano fuorvianti riguardo ai fatti".
- Ad esempio: "Una diagnosi errata di una condizione medica viene mantenuta come informazione all'interno della cartella clinica di un paziente, anche dopo che la diagnosi è stata rettificata, perché è rilevante ai fini della spiegazione del trattamento dato al paziente o di ulteriori problemi di salute'

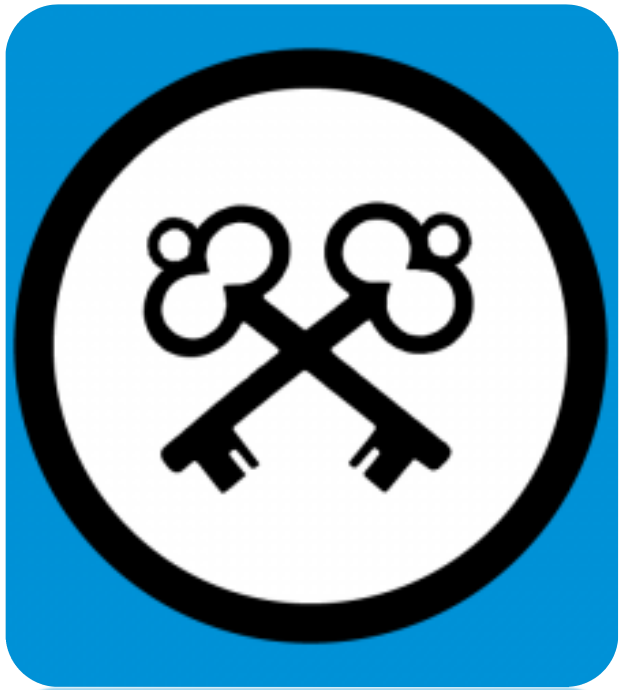
Fonte: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/

PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

- Il GDPR non stabilisce alcun periodo minimo o massimo per la conservazione dei dati personali ma non devono essere conservati per un periodo superiore a quello necessario per tale scopo o per tali finalità.

PRINCIPIO DI INTEGRITA’ E RISERVATEZZA

- i dati dovranno essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.



BUSINESS ASSURANCE

GDPR – Requisiti principali

20 March 2018

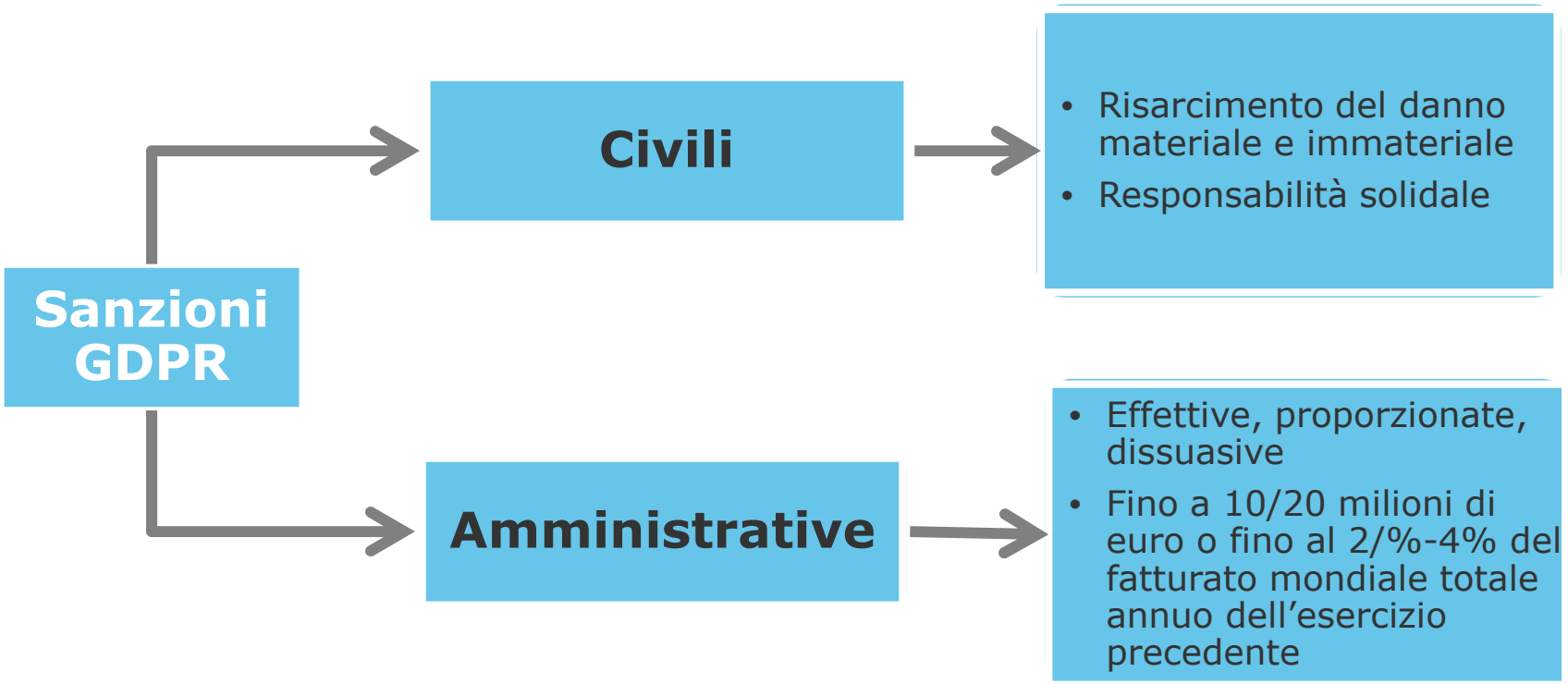
Commercial in confidence

GDPR - THE BIG PICTURE
SUMMARY OF KEY REQUIREMENTS

IMPIANTO SANZIONATORIO

Sanzioni fino al 4% del fatturato o a 20 ML €

NUOVO IMPIANTO SANZIONATORIO



LE SANZIONI AMMINISTRATIVE PECUNARIE

1. Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite **fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo**.

   Ad esempio:

   - la violazione dell'obbligo di tenuta del registro dei trattamenti;
   - la mancata valutazione d'impatto DPIA;
   - l'omessa consultazione preventiva dell'Autorità;
   - l'omessa notifica di data breach;
   - l'omessa nomina del DPO;
   - l'omessa adozione di misure di sicurezza adeguate.

LE SANZIONI AMMINISTRATIVE PECUNARIE

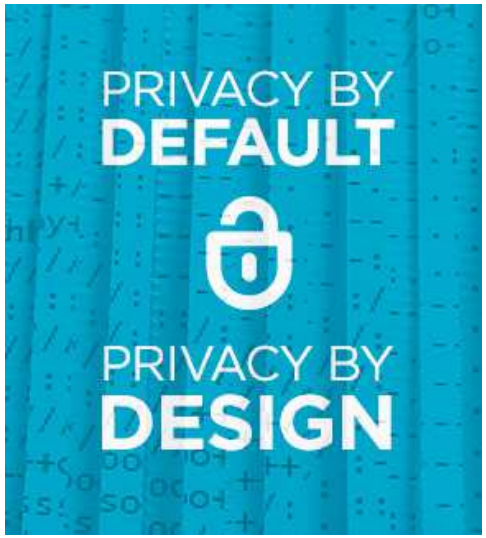
2. Gli altri 29 articoli puniscono **fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo** la violazione dei principi del regolamento e dei diritti degli interessati.

Ad esempio:

- i principi di base del trattamento, comprese le condizioni relative al consenso;
- i diritti degli interessati;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

- Al fine di poter dimostrare la conformità con il presente regolamento il titolare adotta politiche interne e attua misure che soddisfano in particolare i principi della protezione dei dati fin dalla progettazione e della **protezione dei dati di default**.
- Questo implica la 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.



OBBLIGO DI NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI

Si stabilisce l'obbligo per tutti i Titolari del trattamento di effettuare la notifica della violazione all'autorità di controllo entro 72 ore ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

NUOVI DIRITTI INDIVIDUALI

Diritto alla cancellazione (diritto all'oblio)

inteso come il diritto dell'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano in presenza di particolari condizioni

Diritto di limitazione di trattamento,

con cui l'interessato può chiedere una restrizione del trattamento

(ad es. la sola conservazione dei dati con esclusione di qualsiasi altro utilizzo)

I diritti dell'interessato

- I diritti dell'interessato al trattamento enumerati nel capo III del GDPR sono:
- il diritto ad essere informato (artt. 12-13-14);
- il diritto di accesso ai dati (art. 15);
- il diritto di rettifica (art. 16);
- il diritto alla cancellazione dei dati, o «diritto all'oblio» (art. 17);
- il diritto alla limitazione del trattamento (art. 18);
- il diritto alla portabilità dei dati (art. 20);
- il diritto ad opporsi a determinate forme di trattamento (art. 21)
- Il diritto a non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei dati che lo riguardano (art. 22).

Il diritto all'informazione - Informativa

- Sinteticamente, l'interessato ha diritto a essere informato in merito:
- all'esistenza di trattamenti di dati personali che lo riguardano;
- alle finalità di tali trattamenti;
- all'identità dei soggetti che svolgono il trattamento (titolari) e dei loro principali collaboratori (rappresentanti e responsabili della protezione dei dati);
- all'identità dei soggetti terzi a cui i dati potrebbero essere comunicati (destinatari), e alla possibilità che i dati siano trasmessi in un Paese extra-europeo;
- al periodo di conservazione dei dati;
- all'eventuale obbligo di comunicare i propri dati e alle conseguenze della mancata comunicazione;
- all'eventuale automatizzazione dei processi di trattamento, alle logiche utilizzate in tali processi e alle possibili conseguenze;
- all'origine dei dati personali (quando non sono stati comunicati dall'interessato stesso);
- ai diritti che l'interessato può esercitare in relazione al trattamento.

Il diritto alla cancellazione: eccezioni e limiti

- L’interessato non ha diritto a ottenere la cancellazione di dati quando il trattamento è necessario:
- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- per l'adempimento di un obbligo di legge previsto dal diritto nazionale o comunitario;
- per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio dei pubblici poteri, da un soggetto investito di tali poteri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità; se si tratta di «dati particolari», il diritto alla cancellazione non sussiste solo se il trattamento è effettuato da o sotto la responsabilità di un professionista soggetto al segreto professionale;
- per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
- per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici se la cancellazione rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento, e purché il trattamento sia soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, e avvenga nel rispetto del principio della minimizzazione dei dati, utilizzando, ove praticabile, la pseudonimizzazione o l’anonimizzazione dei dati.

DATA PORTABILITY

GDPR introduce la **data portability.**

Il Diritto alla portabilità dei dati, definito "il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e di trasmettere tali dati a un altro titolare senza impedimenti"

CONSENSO

SPECIFICO E INFORMATO

Un consenso per ogni finalità

Preceduto dall'informativa

DIMOSTRABILE

Il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali (onere della prova)

FACILITÀ DI REVOCA

ESPLICITO

Solo per il trattamento dei dati particolari e per la profilazione

All'interno di un contratto scritto la richiesta di consenso deve essere presentata in modo chiaramente distinguibile e con un linguaggio semplice e chiaro.

Il consenso diviene più severo

- diritto di revoca del consenso
- consensi separati per diversi trattamenti
- trattamento legittimo senza consenso

Minori

- I minori meritano una specifica protezione relativamente ai loro dati personali
  - vi è trattamento lecito per i dati di un minore, se questi a 16 anni
  - Se l'età è inferiore ai 13 anni si necessita dell'autorizzazione genitoriale

ACCOUNTABILITY

Per il GDPR Deve essere dimostrata la sostanza degli adempimenti non il rispetto formale. Non basta aver adempiuto alle richieste normative, ma occorre essere in grado di DIMOSTRARLO.

Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento" (art. 24)

Le figure previste dal GDPR

"Accountability e Responsability "

Titolare del trattamento

- Responsabile dell'applicazione del GDRP
- Sanzioni fino a 20 mln o 4% del fatturato

Responsabile del trattamento

- Incarico con contratto vincolante
- Istruzione documentata
- Assiste il titolare

Persone autorizzate al trattamento

- Esecutori materiali delle attività di trattamento

RPD o DPO

- Responsabile Protezione dati personali (non è il responsabile del trattamento)

OBBLIGO DI NOMINA DELLA FIGURA DEL DPO

Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

Tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati SU LARGA SCALA;

Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici o di dati relativi a condanne penali.

I COMPITI DEL DPO

Informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

Verificare l'attuazione e l'applicazione del Regolamento nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

Fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

Fungere da punto di contatto per gli interessati;

Cooperare e fungere da punto di contatto per l'Autorità di controllo

NUOVO AMBITO DI APPLICAZIONE TERRITORIALE

Il regolamento si applica al trattamento di dati personali effettuato da un Titolare o da un Responsabile stabilito nell'Unione anche se il trattamento è effettuato fuori dall'Unione

Il regolamento si applica al trattamento dei dati personali di residenti nell'Unione Europea effettuato da un Titolare o da un Responsabile anche non stabilito nell'Unione Europea, quando le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai cittadini residenti nell'Unione Europea
- il controllo del loro comportamento nell'Unione

RISK BASED APROACH

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

DATA PROTECTION IMPACT ANALYSIS

Quando un tipo di trattamento, in base alla natura, l'oggetto, il contesto e le finalità del trattamento, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.**

La valutazione d'impatto unitamente all'obbligo di tenuta dei registri sostituisce l'obbligo di generale di effettuare la notificazione all'autorità di controllo e si inserisce nel principio di *accountability*.

Si riconferma la scelta del regolamento di strategie di tutela sostanziale e non formale.

Se a seguito della valutazione d'impatto permangono rischi elevati il titolare deve richiedere una **verifica preliminare** all'autorità.