Breve Guida ai concetti fondamentali

General Data Protection Regulation
UE 2016/679

Regolamento Generale sulla Protezione dei Dati

Introduzione

Dopo tanta attesa, lo scorso 4 maggio 2016 (in vigore dal 25 maggio) è stato pubblicato in Gazzetta Ufficiale Europea il Regolamento Generale per la Protezione dei Dati (o GDPR - General Data Protection Regulation UE 2016/679) con efficacia definitiva (e scadenza per eventuali adeguamenti) il 25 maggio 2018.
Si tratta di un Regolamento attraverso il quale la Commissione Europea si pone lo scopo di rafforzare ed omogeneizzare tra tutti gli stati membri dell'Unione Europea la protezione e il trattamento dei dati personali delle persone fisiche (cittadini), oltre che a disciplinare il tema della circolazione dei dati, obbligando quindi tutti i Titolari del trattamento dei dati (anche con sede legale al di fuori dell'UE) che trattano dati di persone fisiche residenti nell'UE ad osservare ed adempiere agli obblighi previsti da tale Regolamento.

Il Regolamento inoltre, dal 25 maggio 2018, andrà a sostituire la Direttiva 95/46/CE e abrogherà la normativa vigente di ciascun Stato membro dell'UE, che nel caso italiano si traduce nell'abrogazione in toto del D.Lgs 196/2003 "Codice per la protezione dei dati personali".
Inoltre, non essendo una "Direttiva", esso non richiede alcuna forma di legislazione applicativa da parte degli Stati membri dell'Unione Europea, diventando, di fatto, efficace alla data sopracitata.

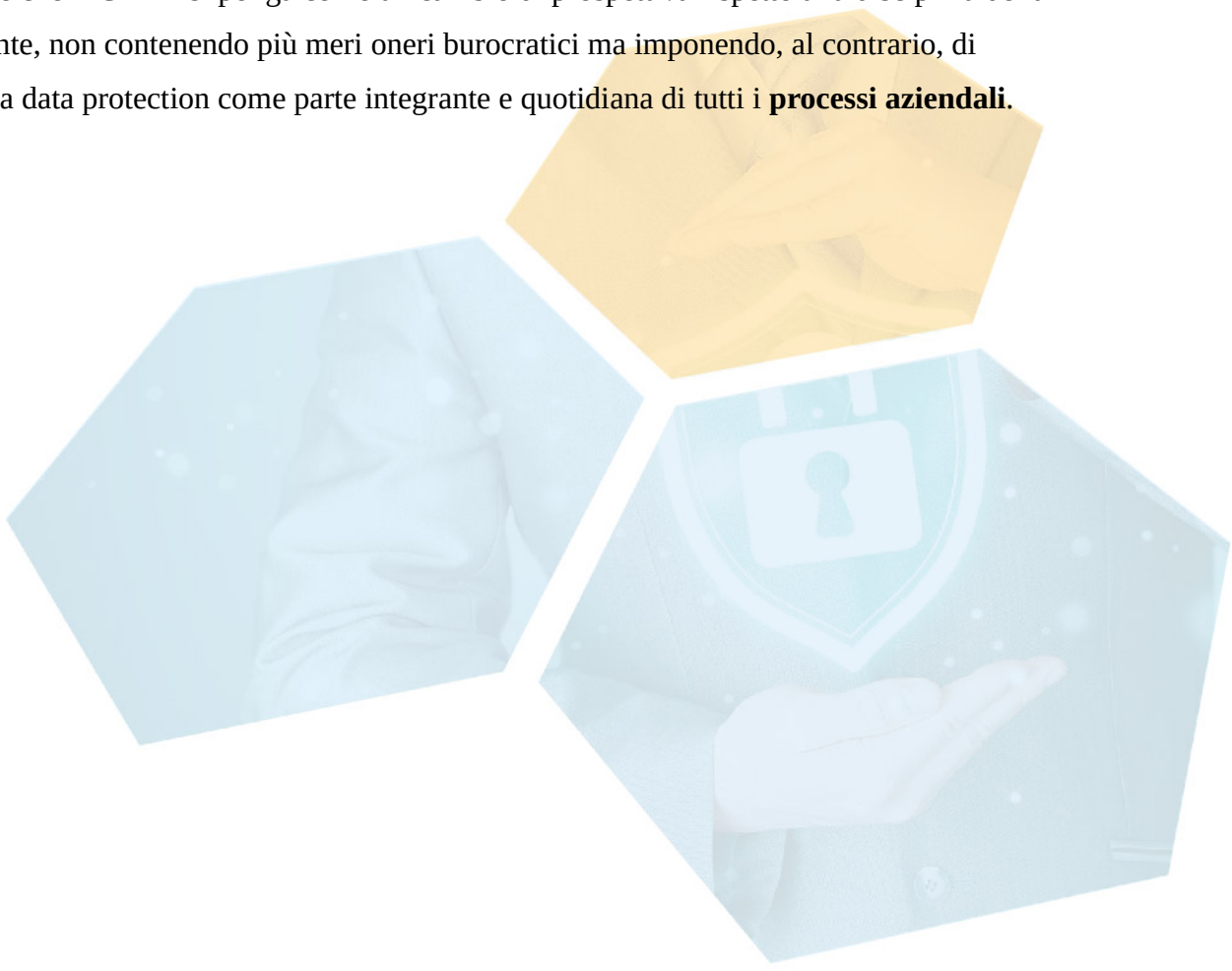
Il GDPR è la "versione europea" di regolamento sul controllo dei dati che si estende ad altre giurisdizioni. Altre normatve simili comprendono il Privacy Act in Australia, l’Ant-Spam Law in Canada, la Cybersecurity Law in Cina et la Personal Data Localizaton Law in Russia.

Il GDPR riprende e sviluppa i concetti classici nel campo della protezione dei dati personali ma introduce altresì alcuni nuovi concetti, che rappresentano un'assoluta novità nel panorama legislativo nazionale ed europeo, tra cui:

- la predisposizione del **Registro dei Trattamenti** a carico dei Titolari, tenendo conto degli obblighi previsti dall'art. 30, che potrà contenere anche ulteriori elementi come l'elenco degli applicativi software utilizzati;
- la stesura e/o modifica della documentazione, come l'aggiornamento delle informative secondo gli ulteriori elementi previsti dal Regolamento, oltre all'introduzione di nuovi documenti, come l'atto di nomina del **DPO** (Data Protection Officer - Responsabile della Protezione dei Dati);

- la definizione di policy di sicurezza ed effettuare la **valutazione dei rischi**, includendo le misure tecniche e organizzative da adottare con riferimento agli obblighi del Titolare del trattamento di garantire (e dimostrare) la conformità rispetto a quando previsto dal GDPR (c.d. principio di "accountability");
- l'obbligo da parte del Titolare di comunicazione all'Autorità Garante tutte le violazioni di dati personali che si siano verificate (c.d. "**data breach**" – es. perdita di dati, violazione di account di posta, furto di identità, ecc...), che implica la definizione di procedure a tale scopo, che siano idonee a scoprire eventuali violazioni verificatesi, generare un'adeguata reportistica e individuare le conseguenze che dalle stesse derivano;
- prevedere la valutazione di impatto di ogni trattamento - **DPIA** Data Protection Impact Assessment - in particolar modo riferita ai trattamenti considerati "a rischio", ad esempio basati su tecnologie molto innovative (smart). l GDPR comunque non specifica quali trattamenti debbano ritenersi a rischio, per cui sarà onere del Titolare compiere una valutazione caso per caso, tenendo conto anche delle indicazioni pratiche fornite dalle linee guida del gruppo di lavoro WP29 dell'Unione Europea.

E' auspicabile che il GDPR si ponga come un cambio di prospettiva rispetto alla disciplina della privacy vigente, non contenendo più meri oneri burocratici ma imponendo, al contrario, di considerare la data protection come parte integrante e quotidiana di tutti i **processi aziendali**.



Domande e Risposte sul GDPR

Cosa devo fare?

Il GDPR impone un diverso approccio alla data protection, superando la logica del "minimo indispensabile" e obbligando le organizzazioni ad essere proattive nell'applicazione di misure idonee ed adeguate in quanto saranno chiamate a dimostrarne l'applicazione in caso di data breach secondo il principio di "accountability".

Cosa cambia per la mia Azienda?

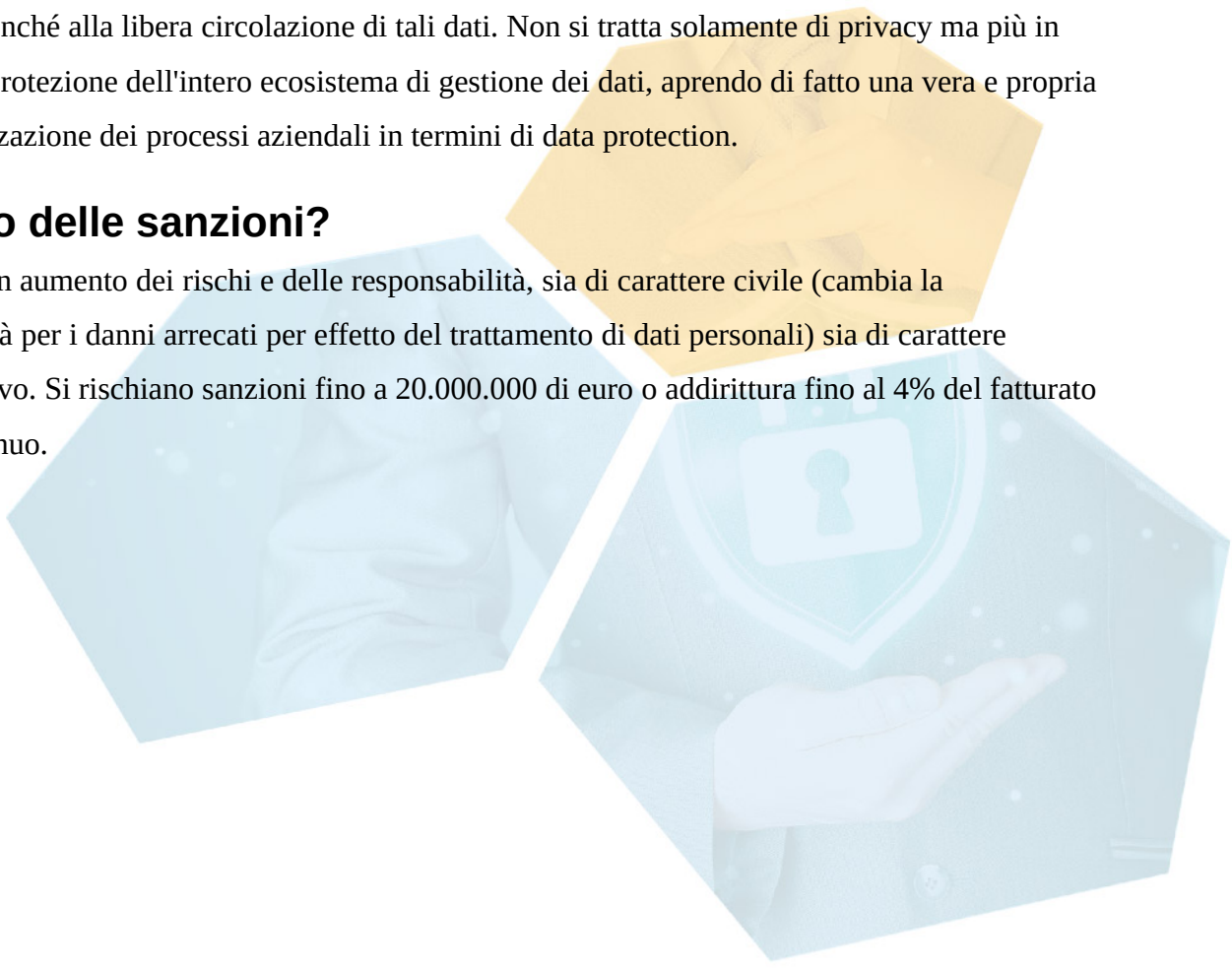
Il GDPR contiene, insieme ad alcune conferme di elementi già noti nel campo della protezione dei dati personali, numerosissime novità: il principio di "accountability", i nuovi parametri connessi alla privacy by design e privacy by default, i registri dei trattamenti a carico dei titolari, il DPIA, le nuove regole sui data breaches e la figura del DPO.

Solo Privacy?

Il GDPR regolamenta la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Non si tratta solamente di privacy ma più in generale di protezione dell'intero ecosistema di gestione dei dati, aprendo di fatto una vera e propria reingegnerizzazione dei processi aziendali in termini di data protection.

Esistono delle sanzioni?

E' previsto un aumento dei rischi e delle responsabilità, sia di carattere civile (cambia la responsabilità per i danni arrecati per effetto del trattamento di dati personali) sia di carattere amministrativo. Si rischiano sanzioni fino a 20.000.000 di euro o addirittura fino al 4% del fatturato mondiale annuo.



Come può aiutarti Next Data

Aspetti generali e normativi

Grazie alle nostre partnership, mettiamo a disposizione i nostri esperti legali in merito a:

- Il nuovo Regolamento UE n. 679/2016 sulla data protection
- Guida Applicativa del Garante Privacy del 28 aprile 2017
- Novità introdotte e differenze rispetto alla normativa nazionale
- Accountability: l'assetto delle responsabilità del Titolare e del Responsabile del trattamento
- I concetti di Privacy by design e privacy by default
- Il registro delle attività di trattamento
- Gli adempimenti in caso di data breaches
- Il DPIA - Data Protection Impact Assessment - e la sicurezza dei dati
- La consultazione preventiva del Garante
- Il rafforzamento dei diritti dell'interessato
- Diritto di accesso
- Diritto di rettifica
- Diritto alla cancellazione ("diritto all’oblio")
- Diritto di limitazione di trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione
- Le Linee Guida sul DPO adottate dal Gruppo Art. 29 il 13 dicembre 2016
- Quando e perché nominare un DPO
- La posizione e i compiti del DPO

Aspetti organizzativi

Ti forniamo supporto e affiancamento nei processi decisionali che riguardano:

- Cosa cambia nei rapporti con soci-persone fisiche e soci-persone giuridiche
- Cosa cambia nei rapporti con fornitori, responsabili esterni al trattamento ed altre figure interessate
- Le sanzioni e le responsabilità
- Il diritto al risarcimento e le responsabilità connesse
- L’aggravamento delle sanzioni amministrative pecuniarie

Aspetti tecnologici

Infine, i nostri esperti tecnici sono consulenti in tema di:

- Endpoint Protection & Encryption
- Cancellazione sicura dei dati
- Backup, backup copy e backup as a service
- Disaster Recovery & Business Continuity
- Security Management & security monitoring

Desideri conoscere la nostra proposta completa in tema di GDPR?

Contattaci al numero 0532 1716257 oppure scrivici a gdpr@next-data.com