Vademecum sul

GDPR

GC Xolution

Via Copernico 36 – Milano

PI e CF 08788640962

Tel 349/8786155

E-Mail
info@gcxolution.com
PEC gcxolution@pec.it
www.gcxolution.com

Vademecum sul GDPR

Introduzione

Dopo un iter durato più di quattro anni, il 4 maggio 2016 è stato pubblicato sulla GUCE il testo definitivo del Regolamento (UE) 2016 n. 679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, altrimenti detto GDPR (General Data Protection Regulation). Esso si avvia a diventare il punto di riferimento normativo ultimo per ciascuno Stato Membro dell'Unione Europea, aprendo di fatto una vera e propria fase inedita in materia di protezione dei dati personali. Il Regolamento sostituirà in toto la Direttiva 95/46 CE, la quale rappresenta dal 1995 – anno della sua approvazione- la Direttiva "madre" a cui ogni Stato Membro dell'Unione ha dovuto riferirsi nel disciplinare internamente la protezione dei dati personali.

Il nuovo Regolamento contiene, insieme ad alcune conferme di elementi già noti nel campo della protezione dei dati personali, numerosissime novità: basti pensare all'introduzione di principi quali quello di accountability o ai nuovi parametri connessi alla privacy by design e privacy by default; e, ancora, all'introduzione dei registri dei trattamenti a carico dei titolari; alla necessità del DPIA – Data Protection Impact Assessment; alle nuove regole sui data breach ossia come agire in caso di violazione di dati personali; alla figura del DPO- Data Protection Officer, sconosciuta al nostro ordinamento. Senza tacere la necessità di un diverso approccio alla data protection, non più "arroccato" sul minimo indispensabile ma proattivamente teso a misure idonee ed adeguate, caso per caso.

Il tutto con un forte aumento dei rischi e delle responsabilità, sia di carattere civile (cambia, e non poco, il regime di responsabilità in caso di danni arrecati per effetto del trattamento di dati personali) sia di carattere amministrativo-pecuniario (come ormai noto ai più, si rischiano sanzioni fino a 20.000.000 di euro o addirittura fino al 4% del fatturato mondiale annuo, se superiore).

La deadline (ma forse sarebbe meglio dire: la start line!) per il recepimento e l'integrale applicazione del GDPR è il prossimo 25 maggio 2018.

Detto quindi che chi comanda è il principio di accountability e che ognuno sarà libero di assumersi le sue responsabilità, abbiamo provato a declinare il da farsi in modo consulenziale, ponendoci, come facciamo sempre, nella stessa condizione del nostro cliente che accompagneremo, in tutto o in parte, in questa avventura.

Vogliamo sottolineare alcune cose prima di partire. Sappiamo bene che non si potrà fare tutto in una volta, e forse neanche tutto in tempo. Bisognerà quindi definire delle priorità. Inoltre sarà opportuno informare di tutto non solo il titolare, e ciò è scontato, ma anche tutti i singoli responsabili del trattamento, ovvero quelli nominati tali in passato o in questa fase contingente: ciò perché, a differenza di quanto previsto dal vecchio codice, l'interessato danneggiato potrà ricorrere indifferentemente nei confronti del titolare o dei singoli responsabili, a seconda di quello che gli pare più semplice e conveniente. Infine, prendiamo atto che, spesso, la molla che fa muovere le imprese e gli enti italiani su questa materia è data dalla paura delle sanzioni, ma siamo e restiamo convinti che la sicurezza dei dati sia come la sicurezza del patrimonio personale: va attuata, e va attuata al meglio: stiamo proteggendo il nostro patrimonio!

Una definizione che va fornita prima di proseguire il discorso è quella di data breach o di Data Protection Violation: si può tradurre genericamente in violazione dei dati. Molto più praticamente possiamo identificare una qualunque violazione, sia essa un furto o un cryptolocker: e questo è molto più vicino alla realtà quotidiana.

Chiudiamo questa introduzione con un piccolo approfondimento sul principio di accountability: cosa significa in pratica? Significa che il legislatore europeo non ci dice più "cosa fare", ma ci fornisce dei principi da applicare. Se andremo in sede di giudizio, sarà il giudice a valutare se avremo applicato al meglio i principi della legge, senza scorciatoie o dimenticanze, sulla base delle best practice e del progresso tecnologico. In sostanza scarica sul titolare e sui responsabili tutta la questione. Stiamo attenti! E' utile ricordare che il Garante paga gli stipendi dei propri dipendenti con le sanzioni che commina a chi cade in fallo…

Cosa fare di sicuro

Le cose che scriviamo ora valgono per tutti: la domanda fondamentale è: il GDPR tocca la mia organizzazione? Ora, fatto salvo che la risposta è facile per le organizzazioni pubbliche di qualunque dimensione, che sono interessate al 100%, abbiamo sentito diversi distinguo tra le aziende. Riconosciamo che la posizione di chi produce parti meccaniche è diversa da chi eroga servizi agli anziani, ma alcune prese di posizione ci hanno spiazzato. Ci siamo sentiti dire da alcuni CIO che le loro organizzazioni non sono di certo sottoposte alla normativa perché non gestiscono in alcun modo dati personali (se si esclude l'elenco dei clienti e dei fornitori, e con paghe esternalizzate). Allora abbiamo chiesto: ma non avete neanche la posta elettronica? E con questa domanda sono andati in

buca. Ora, noi non abbiamo la presunzione di verità, ma una certa esperienza possiamo vantarla. Nonostante questo riteniamo indispensabile partire con un servizio di consulenza legale, che serve a circoscrivere gli adempimenti ed il chi deve fare che cosa ed il chi fa cosa in modo determinato. A tal fine la nostra collaborazione pluriennale con lo studio legale Orlandi & Partners è garanzia di professionalità e certezza della corretta interpretazione del diritto.

Riportiamo lo stralcio di una intervista rilasciata da Stefano Orlandi al Corriere della Sera:

CORRIERE IMPRESE
EMILIA-ROMAGNA
UOMINI, AZIENDE, TERRITORI

C

I mestieri del futuro

Cloud, internet delle cose e big data stanno stravolgendo il modello produttivo come lo conosciamo. Ma sulla via Emilia stanno già nascendo nuove professioni: dal guardiano della privacy al fundraising manager, dall'agricoltore idroponico al personalizzatore di farmaci. Biffi (Unibocconi): «Chi non si adatta soccomberà»

gradino più alto del podio qui in regione. Dall'articolo del 1° maggio i nostri lettori sanno che si tratta di Caffeina: «un'agenzia digitale creativa fondata da tre ex studenti dell'Università di Parma a fine 2011». Ebbene, essa occupa l'87esima posizione nella graduatoria generale, è l'unica delle emiliane nella Top100 ed è cresciuta del 1.092% nel periodo considerato. Molte sono le specializzazioni che caratterizzano, lungo la Via Emilia, le 20 «aziende siluro».

continua a pagina 15

...continua

Protettore della privacy

«Serviranno 30.000 figure in Italia I dati personali sono il nuovo petrolio»

A metà tra il giurista e l'esperto di informatica, il data protection officer (responsabile della protezione dei dati) diventerà una figura obbligatoria per decine di migliaia di aziende a partire dal 25 maggio 2018, con l'applicazione del regolamento europeo per la protezione dei dati personali approvato l'anno scorso. Riguarderà amministrazioni pubbliche, soggetti la cui attività principale consiste in trattamenti che richiedono il controllo degli interessati, enti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili. Ma c'è chi in materia di privacy opera già da vent'anni: «Ho iniziato a lavorare su questo tema nel 1996, quando è stata varata la prima legge — spiega l'avvocato bolognese Stefano Orlandi —. Chi ha questa funzione deve avere competenze incrociate tra diritto e tecnologie». E dovrà occuparsi di supportare le aziende nella protezione dei dati trattati, oltre a raccordarsi con i portatori di interessi esterni. Orlandi segue il modo in cui vengono trattati i dati personali dei clienti, che non se ne abusi, che non vengano messi a rischio (per esempio con le diagnosi dei pazienti delle aziende sanitarie).

È una figura che già molte aziende prevedono, ma che in futuro, con l'attuazione del regolamento, avrà sempre più spazio: «Serviranno tra le 20 e le 30 mila figure solo in Italia», stima Orlandi. Ma il salto potrebbe anche essere più grande: «C'è un passaggio culturale da valutare: bisogna vedere se ci si limiterà alle aziende obbligate o se diventerà una figura richiesta anche da quelle che non sarebbero costrette dalla normativa». In ogni caso, per gli avvocati, è uno sbocco professionale in più: «Ormai è evidente, il nuovo petrolio sono i big data: c'è sempre più interazione tra business, dati e tecnologie — riflette l'avvocato —. Incrociando questo dato di fatto con l'introduzione della nuova norma europea, il responsabile per la protezione dei dati avrà molto peso nei prossimi anni».

Legale Stefano Orlandi

R. R.

E la via Emilia guarda già avanti

Cosa fare obbligatoriamente

C'è chi si chiederà che differenza c'è fra il "cosa fare di sicuro" ed il "cosa fare obbligatoriamente". Possiamo dire che dopo aver definito chi rientra e come rientra nell'applicazione del dettato normativo si saranno alcuni adempimenti ai quali ottemperare con certezza. In particolare.

Redazione DPIA Data Protection Impact Assesment: si tratta della redazione di un documento volto a predisporre la valutazione dell'impatto sulla protezione dei dati personali (DPIA) dei trattamenti di dati che lo richiedano, in base all'art. 35 del GDPR.

Istituzione della figura del DPO: si tratta di una figura singola o di un team multidisiciplinare, che può anche essere individuata all'esterno dell'organizzazione del titolare e disciplinata da un contratto di servizio, che:

- Lavora in staff con il top management
- E' il garante interno, nominato dal responsabile del trattamento, ovvero il titolare
- Lavora in autonomia: non può prendere istruzioni dal titolare
- Deve avere competenze specifiche ed effettuare segnalazioni e report del suo operato di controllo, ma non ne è responsabile. Il responsabile è sempre il titolare

Ethical Hacking: se consideriamo il ciclo di vita della sicurezza come circolare, a fronte di ogni azione/ inazione, dobbiamo valutarne l'efficacia. In ragione di ciò un controllo periodico, che noi chiamiamo servizio di security plus, volto a monitorare la sicurezza esterna ed interna, e l'integrità organizzativa dell'Active Directory (stato rete, utenti, password, dominio).

Encryption dei dati: Non c'è obbligatorietà ma va considerata come misura da implementare per rafforzare l'accountability, e noi la inseriamo di default fra le cose da fare. Infatti, nel caso di violazioni di dati personali che sono stati preventivamente criptati non c'è obbligo dinotifica dell'eventuale data breach al Garante; in caso contrario la notifica deve essere fatta entro 72 ore dall'avvenimento del fatto, con una sorta di autodenuncia. Non ci sembra un bel biglietto da visita…

Anti Ramsomware: I ramsomware non sono virus e stanno diventando pervasivi: sono necessari moduli specifici per ridurre il rischio di criptazioni dei dati non volute.

Cancellazione sicura dei dati: la cancellazione dei dati in modo sicuro è prevista dall'art. 17 del GDPR. 3CiME offre prodotti o servizi per la soluzione definitiva del problema. Non basta più, per fortuna dell'umanità diciamo noi, mettere un chiodo sugli hard disk o nastri. Dobbiamo avere in mano un certificato che dimostri, in modo opponibile ai terzi, che i dati sono stati definitivamente cancellati dai nostri supporti, ed è ora che smettiamo di inquinare il pianeta con immondizia informatica. Vogliamo diventare green e donare, con la formula anglosassone della "charity" computer e server a scuole o associazioni no profit che non hanno risorse economiche per comprarseli. E' ora di invertire la rotta.

Disaster Recovery: Il DR non è solo un obbligo: è necessario per il buon senso dell'attività imprenditoriale. E non ci sono solo i terremoti, ma anche altre sventure posso colpire i nostri dati. Il DR non è il back-up!

Business Continuity: La continuità operativa è un sostanziale risparmio di costi: le macchine si fermano, si rompono, ma le organizzazioni devono poter lavorare con valori del 99,999%. La non continuità operativa comporta un rischio di perdita e danneggiamento dei dati, ed è quindi un sostanziale obbligo.

E per chi ha migrato qualcosa in **cloud**, sia essa posta o altro: conformemente alle linee guida del Garante italiano e della Commissione UE, si chiede a chi va in cloud (sia esso Amazon, Microsoft, Lepida, Google, ovvero con una società che gestisce datacenter) di avere una copia dei dati *"nelle mani" del titolare*, con varie finalità tra cui l'exit strategy.

Cosa fare di caldamente consigliato

Ci sono altri aspetti che rendono l'organizzazione certamente più "compliant". Non si possono di certo considerare obbligatori, ma aiutano, anche perché la materia della sicurezza informatica diventa sempre più complessa da gestire, soprattutto all'interno delle organizzazioni meno articolate. E sempre più non si acquistano prodotti, ma servizi! In particolare ancora una volta.

Security management: è un servizio in outsourcing che gestisce la sicurezza a livello perimetrale, attraverso la completa gestione del firewall e delle sue features.

Backup e backup gestito: Il backup aziendale va semplificato e magari gestito in outsourcing: troppo spesso non lo controlliamo e speriamo che vada tutto bene. 3CiME offre questo servizio già a molti clienti.

Autenticazione federata: abbiamo visto orrendamente replicare il proprio Active Directory in Azure. È come dare le chiavi dei nostri dati all'esterno. Molto più conformemente si può federare i sistemi di autenticazione aziendale con quelli esterni, siano essi Office 365-Azure che Amazon o Google.

Cosa fare opzionalmente a secondo della mia organizzazione

Ci sono altri punti che possono aiutare nella quotidianità della gestione di un problema che non è certo il "core" dell'organizzazione e che non devono essere dimenticati. Citiamo

Cloud: abbiamo visto contratti cloud che rasentano la illegittimità, più che la non rispondenza al dettato del GDPR oggi, e della normativa italiana prima. Il consulente predispone e/o verifica la contrattualistica dal punto di vista "privacy" e GDPR

Gestione adempimenti GDPR: Gestire tutti gli adempimenti fondamentali del GDPR, inclusi: registro trattamenti, DPIA, data breach, gestione info e consensi, ecc, può aiutare nel non "dimenticare qualcosa"

Le sanzioni

Un ultimo paragrafo lo dedichiamo alle sanzioni che rischiano le aziende e gli enti pubblici che vengono trovati inadempienti:

- Fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione (fra l'altro) degli obblighi del titolare del trattamento e del responsabile del trattamento

- Fino a 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione (fra l'altro) dei principi di base del trattamento, comprese le condizioni relative al consenso, dei diritti degli interessati, delle regole sui trasferimenti di dati personali a un destinatario in un paese terzo

Sono numeri importanti, per le nostre organizzazioni e che nessuno si può permettere!