Il GDPR - General Data Protection Regulation – in breve

Il Gdpr è il General data protection regulation, il nuovo regolamento europeo in materia di protezione dei dati personali operativo dal 25 maggio dopo essere stato approvato due anni fa. Il regolamento n. 2016/679 fa parte del cosiddetto "Pacchetto protezione dati" dell'Ue e introduce una serie di nuove garanzie per i cittadini europei o ne rafforza di già previste, riordinando i precedenti provvedimenti in materia di privacy. In quanto regolamento, interviene in modo diretto nelle legislazioni dei Paesi membri: vale infatti ovunque e non ha bisogno di leggi di recepimento, sebbene necessiti di un lavoro di armonizzazione con le proprie leggi, per evitare cortocircuiti. Proprio come accaduto in Italia. Ma a chi si applica, cosa prevede, quali sono le novità? Eccole spiegate per punti.

A chi si applica il GDPR.

Riguarda persone, società e organizzazioni che raccolgono e gestiscono qualsiasi tipo di dato personale in Europa. Anche se non è necessario che quel trattamento avvenga proprio nel perimetro dei 28. Si va da quelli per l'organizzazione interna delle risorse umane a quelle che, invece, coi dati ci fanno affari, come il caleidoscopico universo del marketing. Inclusi, ovviamente, i colossi (quasi del tutto) statunitensi dell'hi-tech, da Facebook a Google, che infatti nelle ultime settimane hanno adeguato le proprie condizioni d'uso e le politiche per la privacy secondo le indicazioni dei 99 articoli del regolamento.

Cosa si intende per dato.

Alla nozione di dato personale (cioè qualsiasi informazione riguardante una persona fisica identificata o identificabile) il Gdpr aggiunge quelli di dato genetico, biometrico e relativo alla salute.

Consenso

Col Gdpr diventa tutto più chiaro ed esplicito in alcune aree specifiche: dati, consenso, responsabilità, sicurezza, controlli e sanzioni. Il consenso alla raccolta e al trattamento da parte degli utenti dev'essere per esempio fornito in forma chiara, con un atto positivo inequivocabile. Sì a una casella da spuntare, no a caselle precompilate, silenzio assenso o altri meccanismi per così dire poco proattivi. L'autorizzazione dovrebbe anche essere spacchettata, cioè richiesta per ogni elaborazione che su quelle informazioni sarà effettuata.

Accesso

I dati devono essere accessibili. Questa novità è molto chiara dalle modifiche delle piattaforme di questi ultimi giorni. Oltre all'accesso se ne può chiedere la rettifica o la cancellazione nonché l'approfondimento delle informative sulle finalità e sulle tecniche di profilazione, sempre garantendo altri diritti come la proprietà intellettuale e il segreto industriale.

Portabilità

Il Gdpr consente, all'art. 20, al soggetto di riutilizzare i propri dati, oggetto di trattamento da parte di un titolare, per altri scopi o su altre piattaforme. Insomma, di portarseli dietro, magari da una piattaforma di foto a un'altra. Questi dati devono essere forniti in formato strutturato e di uso comune, leggibile da dispositivi automatici e soprattutto interoperabile, cioè in grado di poter essere memorizzato su un dispositivo personale ed eventualmente traslocati altrove. Anche sui social. In futuro dovrebbe ad esempio esser possibile trasferire i dati da un servizio come Instagram ad uno come Snapchat o da Dezeer a Spotify.

La notifica.

Ogni violazione dei dati dev'essere notificata con una serie di informazioni specifiche agli interessati entro 72 ore, dice l'art. 33 del regolamento (cosa che per esempio Facebook non ha fatto nel caso Cambridge Analytica), viene istituito un registro delle attività nel quale vengano registrati nome e dati di contatto del titolare del trattamento, le finalità, le categorie di interessati e di dati raccolti, i trasferimenti di quegli stessi dati verso Paesi terzi o altre organizzazioni, i termini per la cancellazione e una sintesi delle misure di sicurezza adottate.

Il GDPR - General Data Protection Regulation – in breve

La sicurezza.

Le norme basilari vanno dalla pseudonimizzazione e la cifratura dei dati memorizzati a una serie di altre categorie come riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento. Come si diceva, il trasferimento a Paesi terzi è consentito solo nel caso in cui vi sia continuità per quanto riguarda questo genere di condizioni.

Il responsabile della protezione dei dati e il controllo.

Il regolamento istituisce la figura del Data protection officer. Si tratta di una figura distinta dal titolare che deve garantire la messa in pratica ("accountability") delle diverse norme previste. In questo quadro rientra la valutazione d'impatto della protezione dei dati e appunto l'istituzione del Dpo, sorta di "watchdog" del titolare. Una verifica interna, ovviamente, perché ogni Paese dovrà assegnare il controllo alle autorità nominate dal Parlamento, dall'esecutivo o da un organismo indipendente, in gran parte già esistenti, come il Garante per la protezione dei dati personali italiano. Spazio anche a una cooperazione fra autorità nazionali in seno al Comitato Europeo, che molto ha lavorato in questi due anni di transizione.

I minori.

L'art. 8 del regolamento prevede che per offrire servizi ai minori di 16 anni sia necessaria un'autorizzazione da parte dei genitori o di un tutore. Anche sotto questo profilo si sono visti molti (e spesso inutili) movimenti da parte delle piattaforme digitali. I Paesi potranno con dispositivi specifici modulare questa soglia senza poterla comunque portare al di sotto dei 13 anni.

Il diritto all'oblio.

Molto diverso da ciò di cui si è parlato negli anni scorsi rispetto a Google e ai motori di ricerca, il diritto all'oblio previsto dall'art. 17 del regolamento consiste in una sorta di cancellazione rafforzata dei propri dati in determinate situazioni. Per esempio quando non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, quando si revoca o ci si oppone al consenso e se non sussiste altro fondamento giuridico per il trattamento. Oppure quando i dati sono stati raccolti in modo illecito o questo venga imposto dal diritto dell'Unione o di uno Stato membro o, infine, se siano stati raccolti quando l'utente era minore. La novità è che la richiesta inoltrata al primo che ha trattato i dati comporta l'obbligo per quest'ultimo titolare di trasmetterla a tutti coloro che li utilizzano o li hanno utilizzati in seguito. Il diritto all'oblio non si applica tuttavia se il trattamento è necessario "per l'esercizio del diritto alla libertà di espressione e di informazione", "per motivi di interesse pubblico nel settore della sanità pubblica", "a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" o se occorre in sede giudiziaria.

Le sanzioni.

Le autorità di controllo possono condurre indagini, ottenere l'accesso alle informazioni e imporre limitazioni al trattamento, così come vietarlo o imporre alcune azioni, tipo la cancellazione. Si inaspriscono le sanzioni amministrative pecuniarie: le multe possono arrivare fino a 10 milioni di euro o 2% del volume d'affari globale in casi – sono solo due esempi – come la violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione o alla mancata o errata notificazione e/o comunicazione di un data breach all'autorità nazionale competente. Oppure fino a 20 e 4% del fatturato in altre situazioni, come l'inosservanza di un ordine imposto da un'autorità o il trasferimento illecito di dati personali ad un destinatario in un Paese terzo. Rimangono dei margini interpretativi a disposizione delle singole autorità nazionali per stabilire l'entità e la gravità delle violazioni.