Gentile cliente/partner,

come ampliamente noto dal mese di maggio 2018 è entrato in vigore il regolamento europeo relativo alla protezione dei dati (GDPR).

ASP Italia ha da tempo intrapreso un percorso di preparazione che si è positivamente concluso nel mese di gennaio 2018 e che continua a rinnovarsi, con l'ottenimento della certificazione ISO/IEC 27001:2022.

Sicuri di fare cosa utile e spero gradita abbiamo predisposto il documento allegato che ritengo possa essere utile per la comprensione dell'argomento e possa tradursi in una guida per gli interventi necessari.

ASP Italia è lieta di poter mettere a disposizione tutta la sua esperienza e competenza per aiutarvi qualora sorgessero dubbi o difficoltà o semplicemente riteniate di volervi confrontare sull'argomento.

Non esitate quindi a contattare il vs. referente o il sottoscritto per qualsiasi informazione.

Un saluto Cordiale

Giovanni longoni

Ceo

Sommario

GDPR: cosa è ?

Si chiama GDPR (General Data Protection Regulation) e rappresenta un importante cambiamento in termini di compliance per tutte le aziende europee, indipendentemente dalle loro dimensioni. Si tratta del nuovo Regolamento Generale sulla Protezione dei Dati, ossia un insieme di norme e linee guida che, a partire dal 25 maggio 2018, tutte le realtà professionali devono rispettare con l'obiettivo di rendere omogenee e rafforzare le modalità di trattamento dei dati personali nella UE.

Il nuovo regolamento europeo rivoluziona il trattamento dei dati personali e la tutela della privacy in ambito professionale. Dal 25 maggio 2018 la norma è applicabile anche a livello sanzionatorio.

Questo significa consolidare le misure per la tutela della privacy seguendo i dettami del GDPR, rispondendo al contempo ad un'esigenza di protezione e sicurezza dei dati sentita a livello globale e legata a doppio nodo all'emergere di minacce informatiche sempre più complesse.

Il nuovo Regolamento si propone di restituire ai cittadini europei il pieno controllo sui propri dati personali, un diritto spesso ostacolato da legislazioni nazionali differenti e da scenari tecnologici che a volte sfuggono all'attuale normativa. Per questo, adottare regole uniformi diventa l'unica strada percorribile. Ecco perché tutte le aziende sono chiamate ad adeguarsi, dimostrando di operare in conformità a quanto previsto dal GDPR.

L'obbligo di osservanza delle direttive è imposto anche alle imprese con sede legale al di fuori del territorio europeo ma che, nella loro attività, si trovano a gestire o trattare dati personali di chi risiede nello spazio UE.

=> Scarica il Regolamento Generale sulla Protezione dei Dati

=> Scarica la guida del Garante Privacy all'applicazione del GDPR

=> Scarica la guida in 12 passi per prepararsi al GDPR

Conformità al GDPR: cosa fare?

Innanzitutto, il regolamento prevede che ogni azienda nomini un Responsabile della Protezione dei Dati (RPD) – nel Regolamento indicato come Data Protection Officer (DPO) - adeguatamente formato per assolvere al compito nel migliore dei modi e a cui spetta l'incarico di fornire informazioni relative alla propria attività ai diretti interessati, siano essi i collaboratori della società, i fornitori oppure i clienti.

Il presupposto di base per un trattamento dei dati personali a norma di legge, infatti, è che l'azienda-titolare del trattamento ne abbia ottenuto il consenso libero, specifico ed informato. Ecco perché il GDPR detta specifiche linee guida al fine di garantire questo fondamentale passaggio, dettagliando quali tipologie di informazioni minime è necessario offrire al soggetto al fine di ottenere il suo consenso al trattamento.

Divise in sei categorie, si tratta di:

- identità del titolare;
- scopo delle operazioni di trattamento per le quali è richiesto il consenso;
- tipo di dati raccolti e trattati;
- esistenza del diritto di revoca del consenso;
- uso dei dati per le decisioni basate su elaborazione automatica (inclusa profilazione);
- nel caso di trasferimento verso paesi terzi, possibili rischi in assenza di garanzie e scelte appropriate.

È poi necessario procedere alla tutela dei dati mediante impiego di crittografia, così da renderli non fruibili a soggetti non autorizzati. Bisogna inoltre garantire che, in seguito a un eventuale problema di natura fisica o tecnica, l'accesso alle informazioni venga ristabilito in modo tempestivo.

Per essere compliant, quindi, si devono rispettare procedure standard di protezione (pseudo- mimizzazione e cifratura dati) e prevedere una valutazione delle misure tecniche e organizzative adottate, che dimostrino la capacità di assicurare riservatezza, integrità, disponibilità, resilienza dei sistemi e dei servizi di trattamento, nonché ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico.

Il GDPR introduce infatti il principio di accountability per tutte le fasi del trattamento. Questo significa adottare soluzioni e strumenti che garantiscano non soltanto la protezione del dato ma anche il controllo, la verifica e l'analisi delle procedure.

Nel caso di una fuga di dati, che si può verificare tramite manomissione, attacco esterno o in modo accidentale, è poi obbligatorio darne avviso tempestivo (entro 72 ore dall'identificazione del problema) all'autorità garante. Eventuali ritardi andranno giustificati.

Per le realtà professionali che contano più di 250 dipendenti vige infine l'obbligo di redigere un registro delle attività con i dettagli sulle policy aziendali attuate in materia di privacy, sulle procedure adottate e sugli standard di sicurezza vantati.

GDPR compliant: come diventarlo?

Al fine di assicurare la conformità a quanto previsto dal GDPR, i passi da compiere sono molti ma imprescindibili. Oltre a contribuire nel centrare gli obiettivi del regolamento, infatti, si eviterà di incappare in sanzioni che, per la mancata compliance, possono arrivare fino al 4% del fatturato.

In ogni caso, è bene non adottare soluzioni improvvisate e avvalersi di consulenti e partner IT preparati e certificati per stilare il piano d'azione migliore e ottimizzare gli investimenti necessari. Se infatti è vero che il GDPR rimette le persone al centro (riconoscendo il pieno diritto alla trasparenza del trattamento dati) è anche vero che tutto questo è ottenibile solo attraverso l'impiego di sistemi e soluzioni altamente affidabili e ad elevato contenuto tecnologico.

Tecnicamente, il primo passo è sostituire le soluzioni di archiviazione locale dei dati con sistemi che centralizzino sia la gestione delle autorizzazioni sia l'accesso ai dati. In altre parole, non sarà più possibile conservare i file esclusivamente su un computer o un disco locale, bensì sarà bene optare per una più avanzata e affidabile soluzione di storage e backup: i sistemi cloud costituiscono a tal fine una delle migliori alternative disponibili, grazie anche (ma non solo) alla ridondanza dei sistemi impiegati.

Affidarsi a fornitori di servizi cloud che certificano la localizzazione all'interno dell'Unione Europea è un'altra scelta possibile, poiché ci si assicura che la gestione delle informazioni avverrà in conformità con il regolamento, nel pieno rispetto degli standard e dei requisiti stabiliti a livello UE.

Lo stesso vale per i Trust Service Provider che si occupano di certificare l'identità digitale mediante strumenti come la firma elettronica o lo SPID (Sistema Pubblico di Identità Digitale).

Pronti al GDPR: entro quando?

Il testo parla chiaro: a partire dal 25 maggio 2018 il GDPR ha definitivamente sostituito le precedenti direttive sulla protezione dei dati. E' dunque scardinato e profondamente modificato uno scenario consolidato da anni, che – complice l'evoluzione del mondo online – risulta insufficiente nel rispondere alle nuove esigenze, non soltanto di privacy ma anche di cyber security.

Come sempre, quando ci si trova di fronte a un cambiamento importante, possono insorgere dubbi legittimi e alcune comprensibili difficoltà. Fortunatamente è possibile contare sul supporto di partner certificati e pronti a mettere le proprie competenze al servizio di chi ne ha necessità.

In tema di piattaforme cloud e soluzioni per lo storage dei dati, a livello europeo il CISPE (Cloud Infrastructure Services Providers in Europe) raggruppa alcuni dei provider che assicurano il pieno rispetto delle regole: L'ottenimento di specifiche certificazioni (es. ISO 27001) garantisce la correttezza dei trattamenti delle informazioni gestite all'interno delle infrastrutture cloud. Importante inoltre ottenere dal provider la garanzia certificata che le informazioni vengono salvate e trattate esclusivamente all'interno dei territori UE/SEE, senza mai essere cedute a soggetti terzi.

Privacy: obbligo DPO in azienda

La nuova figura del Data Protection Officer (DPO): ruolo, responsabilità ed obblighi per le aziende connessi alla nomina del Responsabile del Trattamento Dati.

Con il nuovo regolamento UE n. 2016/679 sulla protezione dei dati nell'Unione Europea, che dal 25 maggio 2018 è applicabile in tutti gli Stati Membri, è stata introdotta la figura del responsabile per la protezione dei dati, o Data Protection Officer (DPO). Il gruppo di lavoro europeo dei Garanti Privacy ha approvato le linee guida del regolamento e la disciplina applicabile al DPO, chiarendone obblighi di nomina, caratteristiche, requisiti, ruolo e responsabilità.

La figura del DPO

Il suo scopo è osservare, valutare e organizzare la gestione del trattamento di dati personali, nonché vigilare sulla loro protezione e sulla corretta applicazione del regolamento UE sulla privacy, ma anche delle norme nazionali sulla privacy, all'interno dell'azienda (pubblica o privata). Il DPO:

- Può essere contattato dal Garante Privacy e dai cittadini in merito al trattamento dei dati personali;
- Deve godere di indipendenza e inamovibilità nello svolgimento delle proprie attività di indirizzo e controllo;
- Ha conoscenza della normativa nazionale ed europea e della legislazione in materia di protezione dati;

In caso di trattamenti non conformi al regolamento europeo, non è personalmente responsabile, diversamente dal titolare e dal responsabile del trattamento (questi ultimi potranno però rifarsi sul DPO per inadempimento del contratto di servizio e chiedere i danni in caso di cattiva consulenza);

La sua funzione può essere svolta anche da un consulente od organizzazione esterni sulla base di un contratto di servizi.

Nomina DPO

La nomina del DPO è obbligatoria per gli enti pubblici e i soggetti privati che effettuano monitoraggio delle persone su larga scala oppure trattano dati sensibili su larga scala. Tra gli esempi forniti dalle linee guida, saranno obbligati a nominare un DPO i Ministeri, le Università, i Comuni, le Regioni, gli ospedali, i sistemi di trasporto pubblico, geo-localizzazione dei clienti di una catena commerciale internazionale, le compagnie di

assicurazione, le banche, i fornitori di servizi di telecomunicazioni, i motori di ricerca che trattano dati a scopi pubblicitari.

Diversamente, non sono obbligati a nominare il responsabile per la protezione dei dati, a titolo di esempio: gli avvocati, il singolo studio medico, le public companies nel settore dei servizi pubblici (energia, ambiente ecc.).

Ulteriori precisazioni arriveranno a breve da parte del Garante italiano per la Privacy, che renderà noto un documento utile a comprendere e utilizzare i nuovi strumenti introdotti dal Regolamento europeo, ad esempio quantificando e rendendo più chiaro il concetto di "larga scala".

Consenso interessato: linee guida WP29

Le linee guida del WP29 sul consenso dell'interessato.

Il 12 dicembre, il Gruppo Articolo 29 (WP29) ha pubblicato la bozza di linee guida in materia di consenso dell'interessato. Il documento vuole fornire maggiori indicazioni a livello interpretativo delle problematiche relative al consenso, anche affiancando ai concetti le esemplificazioni più adatte o ricorrenti nei casi concreti. In questo contributo si cercheranno di affrontare le tematiche principali.

Il presupposto di partenza è che il consenso vada considerato come la base giuridica più appropriata per giustificare il trattamento dei dati personali, proprio per questo soggetta a requisiti rigorosi in quanto deve garantire e dimostrare la genuinità dell'accettazione e del rifiuto. Tuttavia, il titolare del trattamento dovrà sempre valutare se – nel caso concreto – egli abbia a disposizione alternative più adatte tra quelle previste all'art. 6.

L'articolo 4, paragrafo 11, stabilisce che il consenso dell'interessato, in modo inequivocabile, deve essere:

- libero;
- specifico;
- informato.

Sono tre requisiti che, come vedremo, si intrecciano l'un l'altro.

Consenso libero

Si ribadisce che è fondamentale tener conto del bilanciamento dei poteri: l'interessato non compie una scelta reale e si sente obbligato a prestare il proprio consenso anche per evitare conseguenze negative nel caso rifiutasse, allora il consenso non potrà essere considerato come valido. Per esempio se il consenso è inserito in una parte non negoziabile di termini e condizioni si presume che lo stesso non sia stato fornito liberamente.

L'utilizzo del verbo "presume" è significativo in quanto il WP29 chiarisce che in circostanze particolari il titolare del trattamento può vincere tale presunzione fornendo prova della libertà con cui è stato fornito il consenso. Il WP29 specifica che se è pur vero che il trattamento risulta necessario per l'esecuzione del contratto (e pertanto giustificato, ciò soprattutto nei rapporti di lavoro), tale ultima espressione deve essere interpretata rigorosamente; deve sussistere infatti un collegamento diretto e oggettivo tra il trattamento e la prestazione e o il servizio.

Consenso specifico

Il consenso non potrà considerarsi libero se utilizzato per giustificare molteplici trattamenti: se un servizio comporta più operazioni di elaborazione o più scopi, il consenso deve essere dato liberamente per ciascuno. Gli interessati devono essere in grado di scegliere a quali scopi acconsentono il trattamento.

Il Gruppo di lavoro individua tre componenti per garantire questo requisito:

- Indicazione esatta dello scopo, come salvaguardia contro l'abuso di trattamento;
- Granularità nelle richieste di consenso;
- Chiara separazione delle informazioni relative all'ottenimento del consenso per le attività di elaborazione dati da informazioni su altri argomenti.

I titolari del trattamento che desiderano utilizzare i dati raccolti per nuovi scopi sono obbligati ad ottenere dagli interessati il nuovo consenso prima di procedere.

Consenso informato

Senza informazioni accessibili, gli interessati non possono prendere decisioni informate e quindi, chiarisce il WP29 "il controllo dell'utente diventerebbe illusorio e il consenso non valido per l'elaborazione". Il Gruppo ha identificato sei categorie di informazioni minime necessarie:

- L'identità del titolare;
- Lo scopo di ciascuna delle operazioni di trattamento per le quali è richiesto il consenso;
- Quali tipo di dati saranno raccolti e trattati;
- L'esistenza del diritto di revocare il consenso;
- Informazioni sull'uso dei dati per le decisioni basate esclusivamente sull'elaborazione automatica (inclusa la profilazione);

Se il consenso riguarda trasferimenti, circa i possibili rischi di trasferimenti di dati verso paesi terzi in assenza di una decisione di adeguatezza / garanzie appropriate.

Va ricordato anche che l'informativa deve essere facilmente comprensibile per la persona media, non contenere dichiarazioni piene di gergo legale, anzi scritta in linguaggio semplice.

Nelle situazioni, poi, in cui emergono "gravi rischi per la protezione dei dati", è richiesto un consenso esplicito: un diverso livello di consenso rispetto a quello ordinario appena sopra descritto. Ci si riferisce in particolare ai dati relativi all'articolo 9 (categoria speciale), ai trasferimenti verso Paesi o organizzazioni privi di una decisione di adeguatezza e al processo decisionale individuale automatizzato (compresa la profilazione).

Il Gruppo di lavoro suggerisce per esempio che il consenso dato attraverso una espressa e formale dichiarazione scritta (firmata dall'interessato) è da considerarsi esplicito. Altre modalità, in particolare nel contesto elettronico, includono il coinvolgimento dell'interessato: compilare un modulo elettronico; inviare una mail; caricare un documento scansionato con firma; registrare una dichiarazione orale, o verificare il consenso tramite un processo di autenticazione a due fasi (come un'e-mail seguita da un messaggio SMS).

Il gruppo di lavoro fornisce importanti indicazioni in merito al mantenimento della prova del consenso. I responsabili ed il titolare del trattamento terranno prova del consenso per tutta la durata dell'attività connessa all'elaborazione dei dati; quando questa termina, la prova del consenso deve essere mantenuta soltanto al fine di adempiere agli obblighi di legge o per stabilire, esercitare o difendere i diritti legali.

Il GDPR obbliga inoltre i responsabili del trattamento a garantire che il consenso possa essere ritirato con la stessa facilità con cui può essere dato, in qualsiasi momento, anche se non necessariamente attraverso la stessa azione. Tuttavia, il gruppo di lavoro osserva che nel contesto elettronico, se il consenso è ottenuto tramite una singola azione (clic del mouse, scorrimento, sequenza di tasti, ecc.) o tramite l'interfaccia di un singolo dispositivo IoT, il ritiro dovrebbe essere possibile attraverso la stessa interfaccia.

Consenso ottenuto ai sensi della direttiva 95/46/CE

Infine, il consenso pre-Regolamento conforme alla legge nazionale non deve essere necessariamente riformulato e riottenuto. Il Gruppo di lavoro riconosce che "il consenso … ottenuto fino ad oggi continua ad essere valido nella misura in cui è in linea con le condizioni stabilite nel GDPR".

Privacy e DPIA: Linee Guida WP29

Gruppo articolo 29, linee guida sulla valutazione di impatto relativa ai dati personali.

Il Gruppo articolo 29 continua nel suo lavoro di redazione e modifica delle linee guida per la corretta applicazione del nuovo Regolamento sulla protezione dei dati personali.

Il 4 ottobre scorso è stato pubblicato l'aggiornamento delle Linee Guida sulla Valutazione di Impatto sulla protezione dei dati personali (Data Protection Impact Analysis) necessario alla corretta applicazione della nuova normativa in tema di privacy.

In primo luogo viene sottolineata la centralità, nel conformarsi alle prescrizioni del Regolamento, dell'approccio basato sulla corretta considerazione del rischio connesso al trattamento dei dati personali e cioè in relazione a quei trattamenti che possono avere conseguenze pregiudizievoli sui diritti e le libertà delle persone fisiche. Il documento fornisce (anche utilizzando molteplici esempi pratici) le indicazioni interpretative necessarie al fine di capire cosa si deve intendere concretamente con DPIA e quando ricorrervi.

Su questo ultimo punto risultano fondamentali due considerazioni:

pur se il Regolamento richiede la Valutazione di Impatto in specifiche situazioni, tuttavia questa deve essere posta in essere ogni qualvolta il titolare ritenga che ci sia il pericolo che i diritti e le libertà degli interessati possano essere posti a rischio (le Autorità nazionali sono chiamate a rendere pubblico un elenco di trattamenti che comunque dovranno essere sottoposti a valutazione);

la DPIA, non va intesa come un'attività una tantum, bensì come un'attività persistente e ciclica.

Il WP29, infatti, chiarisce come la DPIA è lo strumento principale per garantire il rispetto da parte del titolare del trattamento del principio di accountability (cioè la responsabilità e la responsabilizzazione del titolare del trattamento connessa alla capacità da parte di quest'ultimo di essere in grado di dimostrare l'efficacia e l'efficienza delle misure adottate).

Di fatto, quindi, l'azienda-titolare del trattamento dovrà porre in essere una prima necessaria valutazione del rischio (che potrebbe essere definita: di base) per svolgere un'analisi dei trattamenti ed una seconda, eventuale, valutazione del rischio (che potrebbe essere definita di approfondimento tecnico) in relazione alle misure di sicurezza da adottare rispetto ai risultati ottenuti.

Da queste considerazioni emerge un'importante conseguenza operativa e cioè che qualora il titolare non ritenga che dai risultati della propria valutazione i trattamenti eseguiti non necessitino di una DPIA (in senso stretto), egli dovrà giustificare per scritto le valutazioni fatte da tenere nel registro dei trattamenti svolti sotto la sua responsabilità.

Al fine di supportare il titolare del trattamento a compiere queste scelte, le Linee Guide forniscono nove criteri di riferimento per capire quando, con molta probabilità, sarà necessario procedere alla DPIA:

- Trattamenti che comportano valutazioni della persona e profilazione (es. rendimento professionale, situazione economica, ubicazione, spostamenti, ecc);
- Decisioni automatizzate con effetti giuridici significativi (es. esclusione da benefici);
- Attività di monitoraggio sistematico (es. raccolti di dati attraverso reti, sorveglianza sistematica in un'area accessibile al pubblico);

- Dati sensibili o dati di natura estremamente personale (es. opinioni politiche o sindacali, condanne penali, cartelle cliniche, ecc.)
- Trattamenti di dati su larga scala (il concetto di larga scala va riferito a: numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata, o persistenza, dell'attività di trattamento; ambito geografico dell'attività di trattamento);
- Combinazione o raffronto di insiemi di dati (es. dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti);
- Dati relativi a interessati vulnerabili (si va dai minori sino ai soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici);
- In generale, infine, tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. lo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento).

Nel ribadire che la pubblicazione della DPIA non costituisce un obbligo formale ai sensi del Regolamento – risultando rimessa alla discrezionalità del titolare – le linee guida rilevano come tuttavia sarebbe opportuno che i titolari valutassero di rendere pubbliche almeno parti della DPIA, quali una sintesi o le conclusioni.

Possiamo pertanto concludere riportando un significativo passaggio del documento in commento:

"La DPIA è uno strumento che consente ai titolari di implementare sistemi di trattamento dati conformi al regolamento, e in taluni casi di trattamento la sua conduzione è obbligatoria. Si tratta di una procedura scalabile che può assumere forme diverse, tuttavia i requisiti basilari di una DPIA efficace sono fissati nel regolamento. I titolari dovrebbero guardare alla DPIA come a un'attività utile e positiva che favorisce l'osservanza dei requisiti di legge".

Registri dei trattamenti

Si tratta, in sintesi, di un adempimento formale che fornisce una prima indicazione rispetto al fatto che il Titolare e il Responsabile operano in conformità al GDPR. In caso di **controlli da parte del Garante per la Privacy**, infatti, probabilmente il registro dei trattamenti rappresenta uno dei primi documenti richiesti.

Tra le indicazioni che il GDPR fornisce alle aziende troviamo le informazioni che i registri dovranno obbligatoriamente contenere, ovvero:

1. nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
6. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

PMI escluse

Ci sono alcuni elementi importanti da considerare, tra cui le **esclusioni** previste per enti e altri organismi con **meno di 250 dipendenti** che:

non realizzano trattamenti che possono presentare un **rischio per i diritti e le libertà** degli interessati;

il **trattamento** risulta **occasionale** e non includa dati di cui all'art. 9.1 o all'articolo 10. (dati particolari e dati personali giudiziari).

In attesa di un chiarimento del Garante rispetto alla definizione di "occasionalità" e "rischio per i diritti e le libertà degli interessati", una possibile chiave di lettura è l'applicazione del principio di "**Accountability**" promosso dal GDPR, ovvero la valutazione obiettiva e concreta dei rischi, per garantire l'adozione delle adeguate ed efficaci misure di sicurezza e privacy.

Nuove regole privacy: suggerimenti per aziende

In vigore il nuovo Regolamento per il trattamento dei dati personali: riflessioni di carattere pratico a beneficio delle imprese.

E' in vigore il nuovo Regolamento per il trattamento dei dati personali (GDPR), dopo la pubblicazione in GUUE. Descrizione e schemi sono da tempo reperibili, ma saranno necessari costanti approfondimenti, a partire dall'impatto concreto della nuova normativa sulle imprese, entro due anni direttamente applicabile in Italia. Il Regolamento apporta modifiche e integrazioni al set di definizioni, di cui le imprese dovranno tener conto cambiando il proprio approccio all'interpretazione della norma. Basta richiamare ad esempio, la nuova definizione di "dato personale" che include esplicitamente elementi come identificatori online e i dati relativi alla ubicazione.

Trattamento dati

Di grande rilevanza è anche la nuova definizione di consenso che viene identificato in qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Questi cambiamenti nelle definizioni andranno a influenzare tanti aspetti del business (da quelli commerciali a quelli più strettamente connessi ai rapporti datore-dipendenti). A titolo di esempio si potrebbe ipotizzare che un semplice flag potrebbe non essere più sufficiente a considerare inequivocabile una manifestazione di consenso. Tanto più che il Regolamento ha innalzato maniera sensibile le sanzioni applicabili, sia in termini economici (multa massima 20 milioni di euro o 4% del fatturato annuo) che penali e civili. Senza contare che sono stati attribuiti alle Autorità di Sorveglianza nuovi e più pervasivi poteri.

Informative

Già da quanto accennato appare evidente come anche la redazione delle informative dovrà essere in parte ripensata: concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (laddove tal tipo di preciso obbligo non è presente nell'attuale normativa). È probabile che le Autorità metteranno a disposizione anche modelli di riferimento.

Compliance

Le imprese dovranno riesaminare la conformità del proprio business alla nuova normativa; garantire con maggiore attenzione il tracciamento (documenti interni, policy, ecc.) delle attività di trattamento; quando necessario, identificare una persona idonea al ruolo di DPO garantendone risorse e indipendenza. Nell'ottica

della rivisitazione dei processi e dei progetti aziendali, le imprese dovranno quindi tener conto dei principi di privacy by design e default, ragionando in termini di compliance privacy fin dall'inizio e per tutto il ciclo. Un aspetto così rilevante che, in determinati casi, sarà necessario procedere a una valutazione di impatto sui dati personali (DPIA) sviluppata in maniera più o meno approfondita a seconda del contesto aziendale di riferimento. Allo stesso modo si giustifica il favore che il Regolamento presta alle imprese che procederanno alla redazione di un Codice di condotta.

Profilazione

Un'altra innovazione che inciderà in maniera trasversale sulle scelte delle imprese è la disciplina dettata in materia di profilazione. Marketing, sicurezza, monitoraggio dei clienti, analisi, controllo: presuppongono spesso un'attività di profilazione. Le imprese che se ne occupano, come core business o per processi aziendali, avranno l'obbligo di fornire comunicazioni particolarmente precise e chiare agli interessati.

Sicurezza

Il Regolamento innalza anche il livello della sicurezza, introducendo un generale obbligo di segnalare eventuali violazioni. Le imprese devono prevedere precisi processi, di difesa e di pronta comunicazione. Vanno per esempio individuati: ruoli specifici e responsabilità, formazione dipendenti e modelli di preparazione. Anche per i responsabili del trattamento, il Regolamento impone nuovi e rilevanti obblighi di conformità, doveri e responsabilità. La nuova disciplina coinvolge direttamente quelle aziende che lavorano come responsabili (i.e. gli outsourcers), ma può anche interessare qualsiasi attività commerciale che impegna un responsabile interno. Responsabili e titolari devono quindi rivedere gli esistenti contratti affinché risultino conformi ai dettami del Regolamento.

Trasferimento dati

Per le PMI che hanno sviluppato il proprio business anche al di fuori dei confini italiani va tenuta in debito conto la disciplina sul trasferimento dei dati. Per le imprese che rimangono in Europa varrà il principio del One Stop Shop: tutte le questioni relative al trattamento dei dati personali potranno far riferimento ad un'unica Autorità di Sorveglianza e cioè quella dove hanno il proprio stabilimento. Il trasferimento verso Stati fuori dell'UE, come anche previsto dalla normativa previgente, è permesso soltanto nel caso in cui lo Stato terzo garantisca un'adeguata protezione, ovvero nel caso in cui venga sottoscritto un accordo internazionale (quale il Privacy Shield con gli USA). Diversamente le aziende dovranno tenere in debito conto i modelli di clausole predisposte dalla Commissione. Per i trasferimenti infragruppo, poi, trova maggior riscontro la necessità di predisporre opportune norme vincolanti d'impresa (BCR).

Va infine ricordato che, sebbene la normativa appena approvata intenda regolamentare tutti gli aspetti del trattamento dei dati personali, rimarranno comunque molti settori da armonizzare, anche in considerazione dei molteplici provvedimenti specifici emessi dall'Autorità Garante in questi anni.

Al fine di aiutare le imprese a entrare nei meccanismi del nuovo regolamento, si segnala la ancora attuale guida in dodici passi, pubblicata il 14 marzo dall'Autorità Garante Inglese per la protezione dei dati personali.

Impatto sulle aziende del nuovo Regolamento Privacy

Nuovo Regolamento Europeo sulla tutela dei dati personali: analisi di tutte le novità e delle principali conseguenze per le imprese.

Il 15 dicembre 2015 è stato definito il testo del nuovo Regolamento Europeo sulla tutela dei dati personali. Dal momento in cui diventerà esecutivo ci saranno due anni per adeguarsi, ma già da subito la nuova disciplina segna un punto di partenza fondamentale per le aziende, perché la natura trasversale della privacy

(da diritto fondamentale a materia di business) avrà un impatto rilevante sulla gestione d'impresa: chi si farà trovare pronto e open minded guarderà il futuro con maggiori certezze, gli altri resteranno in coda.

Novità per le aziende

Il Regolamento prevede un unico insieme di norme valide in tutta l'UE, applicabile anche alle aziende extra-europee che offrono servizi o beni nel mercato europeo. Tale uniformità, nel garantire un'applicazione coerente delle norme di protezione dei dati in tutta l'UE, è stata pensata anche per incoraggiare le imprese ad una maggiore concorrenza leale ed a renderle maggiormente partecipi del mercato unico digitale.

Particolare rilevanza è data, sotto questi aspetti, al meccanismo del c.d. one-stop-shop, che permetterà ad una società attiva in più Stati membri di trattare solo con l'Autorità Garante dello Stato in cui ha il proprio stabilimento principale; con la conseguenza, in caso di controversie, di prevedere una sola decisione applicabile a tutto il territorio dell'Unione, riducendo i costi per la risoluzione di tali questioni e fornendo maggiore certezza del diritto.

Conformità

Sotto l'aspetto del trattamento dati, il Regolamento fonda la propria struttura applicativa su un approccio basato sul rischio, con particolare riferimento alla necessità del Privacy Impact Assessment: i titolari del trattamento dovranno essere in grado di implementare le misure di sicurezza tenendo conto dei risultati dell'analisi del rischio relativo alle operazioni di trattamento dei dati svolte all'interno dell'azienda. Proprio per tali ragioni, la nuova disciplina ha tenuto ben presente che diverse aziende svolgono differenti attività e rischi connessi alle stesse, che in termini di privacy possono variare di caso in caso. Un elevato rischio comporterà obblighi più stringenti. I titolari del trattamento dovranno attuare, quindi, tutta una serie di misure tecniche ed organizzative al fine di garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato in conformità al Regolamento; nel caso in cui, per esempio, si verifichino determinate ipotesi di c.d. data breach, ai titolari del trattamento saranno applicate specifiche e stringenti prescrizioni.

Responsabilità

Sotto il profilo della responsabilità, il Regolamento ha esaltato l'importanza dei concetti di privacy by design e privacy by default, come anche dell'importantissima figura del Data Protection Officer, figura che necessiterà di un percorso formativo adeguato e di alto profilo (anche perché per le Pubbliche Amministrazioni e le aziende che trattano dati particolarmente sensibili il DPO sarà obbligatorio). In caso di particolari violazioni le persone interessate, a certe condizioni, potranno presentare denunce presso un'Autorità Garante o proporre un ricorso giurisdizionale con esiti che per i quali i responsabili del trattamento potrebbero affrontare multe massime fino a € 20 milioni o 4% del loro fatturato annuo globale.

Sotto il profilo del trasferimento di dati personali al di fuori dell'UE, il Regolamento stabilisce che questo può avvenire a condizione che un certo numero di prescrizioni e garanzie vengano soddisfatte. Nuove decisioni di adeguatezza (si ricorda la recentissima problematica sul safe harbor) dovranno essere tra l'altro riesaminate almeno ogni quattro anni. Il Regolamento prevede poi che nel caso di rispetto di clausole rispondenti al modello UE non sarà necessaria una specifica autorizzazione da parte dell'Autorità Garante. Infine va rammentato che il Regolamento riconosce ufficialmente BCRs come un meccanismo valido per trasferire i dati personali al di fuori dell'UE.

Privacy su dati commerciali: Codice e diritto oblio

Codice deontologico del Garante Privacy: diritto all'oblio per società di due intelligence che raccolgono dati sulle informazioni commerciali negative degli imprenditori.

Con il *"Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale" promosso* dal **Garante della Privacy** viene ripristinato il **diritto all'oblio** sulle **informazioni commerciali negative** memorizzate nei database dalle società di *due diligence*. Il **Codice deontologico** redatto insieme a varie associazioni di categoria, imprenditoriali e dei consumatori interessate al settore, è disponibile online (pubblicato in Gazzetta Ufficiale n. 238/2015).

Cancellazione dopo 10 anni

Tra le linee guida c'è anche l'**obbligo di rimozione dopo 10 anni** delle notizie su ipoteche, pignoramenti, fallimenti o altre procedure concorsuali contenute nelle apposite banche dati gestite da alcune società private, che forniscono tali informazioni a pagamento (basti pensare ai dati ai quali accedono le società finanziarie nel momento in cui si chiede un mutuo o un prestito). Banche dati che contengono **informazioni** patrimoniali, **economiche**, finanziarie, creditizie, industriali e **produttive** che finora rimanevano memorizzate per un tempo indefinito, in palese violazione della privacy e del diritto all'oblio.

Il limite dei 10 anni si applica a tutte le informazioni commerciali riferite a persone fisiche provenienti da elenchi e registri pubblici, elenchi e informazioni pubblicamente accessibili. Fanno eccezione i dati sensibili e i dati giudiziari, tranne quelli provenienti da fonti pubbliche o pubblicamente e generalmente accessibili da chiunque.

Informazioni nei database

Il Codice deontologico legittima le società di *due diligence* a utilizzare i dati ottenuti da **fonti** pubblicamente e generalmente **accessibili** quali le testate giornalistiche cartacee o digitali, gli elenchi telefonici, i pubblici registri, le sentenze, i provvedimenti giudiziali, gli elenchi, i documenti pubblicamente accessibili, i da siti web di enti pubblici o altre autorità di vigilanza e controllo. Questi dati possono essere trattati **senza consenso** degli interessati, nel rispetto di quanto previsto dal **Codice Privacy**. Possono inoltre essere utilizzati i dati personali che il soggetto stesso ha liberamente deciso di comunicare al fornitore di informazioni commerciali.

Vincoli

Gli operatori sono inoltre obbligati:

- ad annotare sempre la **fonte** da cui hanno tratto i dati personali sulla persona censita;
- a pubblicare un'**informativa** completa almeno sul proprio sito web;
- a verificare la **pertinenza** dell'informazione memorizzata, aggiornando periodicamente i propri archivi (ad esempio per verificare l'intervenuta assoluzione di un soggetto indagato);
- adottare misure per garantire la **sicurezza,** l'integrità e la riservatezza delle informazioni commerciali.

Luci e ombre del Privacy Shield

Garanti Privacy prudenti sul Privacy Shield: nel dopo Safe Harbor, per le aziende è meglio ricorrere alle Binding Rules finché non cadranno i veli sul nuovo accordo.

Unione Europea e Stati Uniti sono riusciti a trovare **nuovi punti di contatto** per risolvere un problema strutturale dell'economia mondiale e del mercato: il corretto trattamento dei dati personali. Saltato l'accordo **Safe Harbor**, in questi mesi le aziende hanno proseguito il loro business ricorrendo alle **Binding Corporate Rules** e alle **Model Contract Clauses**, seguendo anche le indicazioni della Autorità Garanti.

Safe Harbor

Con **sentenza** 6 ottobre 2015, la Corte di Giustizia Europea ha invalidato l'accordo Safe Harbor, che presupponeva gli Stati Uniti "un porto sicuro" per il corretto trattamento dei dati. Per la Corte, infatti, la Commissione non poteva vincolare gli Stati Membri a un tale tipo di accordo, tanto più che – a seguito delle vicende legate al caso Snowden e Schrems – è emerso in modo evidente come la politica di tutela della privacy in territorio americano da una parte, e la sistematica azione di controllo di massa del governo statunitense dall'altra, non possono garantire il rispetto della normativa UE in materia di trattamento dei dati personali.

Privacy Shield

A seguito del nuovo accordo, il Commissario europeo Jourova e il vicepresidente della Commissione Europea Ansip si sono dichiarati molto soddisfatti:

*"Le nostre imprese, soprattutto quelle più piccole, avranno la **certezza del diritto** di cui hanno bisogno per sviluppare le loro attività attraverso l'Atlantico….[n.d.r. questo accordo] ci aiuta a costruire un mercato unico del digitale in Europa, un ambiente online affidabile e dinamico", ha affermato Jourova.*

Ansip ha anticipato invece che gli Stati Uniti si sono impegnati affinché:

*"l'accesso da parte delle autorità pubbliche per motivi di sicurezza saranno soggette a chiari **limiti**, garanzie e meccanismi di **controllo**".*

Quel che si sa del nuovo accordo, infatti, è che riguarderà obblighi sul trattamento dati, meno sorveglianza di massa, diritto al ricorso e difensore civico.

- Le aziende statunitensi che importano dati personali dall'Europa dovranno rispettare **obblighi più stringenti** sul loro trattamento e direttive delle Autorità Garanti Europee. Il Dipartimento del Commercio USA vigilerà che tali aziende rendano pubblici gli impegni presi, la Federal Trade Commission (FTC) agirà affinché gli impegni siano rispettati ai sensi del diritto statunitense.
- L'accesso ai dati da parte di Autorità Pubbliche e Forze dell'Ordine giustificate da ragioni di sicurezza nazionale sarà soggetto a limitazioni, garanzie e meccanismi di controllo. Tali azioni invasive saranno ammesse solo se necessarie e in misura proporzionata. **Vietata la sorveglianza di massa** indiscriminata. Al fine di monitorare regolarmente gli impegni, sarà attuata una revisione annuale congiunta tra UE-USA.
- E' prevista una protezione più efficace dei diritti dei cittadini UE, prevedendo diverse possibilità di ricorso. Le Autorità Garanti potranno presentare casi al Dipartimento del Commercio e FTC. Per i **reclami** nei casi di accesso da parte delle autorità di intelligence nazionali, verrà creato un nuovo **difensore civico**.

Ora dalla teoria e dal mero "impegno" occorrerà passare ai fatti e farlo in tempi ragionevolmente brevi.

L'ottimismo è comprensibile ma ci sono ancora molte **ombre** che incombono. In primo luogo, è da sottolineare come le Autorità Garanti per il trattamento dei dati personali (riuniti nel Gruppo di Lavoro **Articolo 29**, che a suo tempo aveva espresso posizioni ferme in merito alle soluzioni cui ricorrere per uscire dallo stallo normativo e commerciale conseguente la dichiarazione di illegittimità del Safe Harbor), non abbiano ancora espresso un **giudizio** definitivo. Il Gruppo ha sottolineato la necessità di conoscere e approfondire, quanto prima, maggiori dettagli in merito all'accordo, in particolare sulle modalità con cui gli Stati Uniti si sono impegnati al **rispetto dei principi** del Privacy Shield.

Dunque, attualmente è ancora valida la scelta per le aziende di ricorrere alle **Binding Corporate Rules**. Questo punto è particolarmente critico perché l'accordo non sembra affrontare il problema che neanche il Safe Harbor risolveva e cioè l'**applicabilità concorrente** tra le BCR ed, ora, il Privacy Shield. Alternativa ancora non passata al vaglio della Corte di Giustizia e che lascerebbe spazio alla possibilità di nuovi **ricorsi**.

In secondo luogo va considerato che gli strumenti e le novità annunciate implicheranno molteplici passaggi, sia legislativi sia di organizzazione strutturale (per esempio in riferimento al sistema dei ricorsi al difensore civico) che non sono, evidentemente di immediata approvazione ed applicazione.

Dati all'estero e imprese: sentenza UE sul Safe Harbor

Nuova sentenza della Corte UE sul Safe Harbor: analisi delle conseguenze sugli accordi commerciali tra imprese italiane e paesi terzi.

Una recente **sentenza** della Corte di Giustizia **UE** è intervenuta in merito al **trasferimento dei dati personali** in un paese **Safe Harbor**, che cioè "garantisce un livello di protezione adeguato" *(approdo sicuro*) al trasferimento di dati da parte di uno Stato Membro dell'Unione Europea. Il pronunciamento potrebbe avere **conseguenze** importanti per le **imprese italiane**, poiché interviene sulla normativa vigente, in base alla quale:

- è vietato il trasferimento di dati personali da paesi UE verso paesi terzi (non appartenenti ad UE o Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein), in base all'*articolo 25, comma 1, Direttiva 95/46/CE*, a meno che tali paesi non garantiscano un livello di protezione adeguato; la Commissione può stabilire tale adeguatezza attraverso una specifica decisione (*comma 6*);
- in deroga a tale divieto, il trasferimento è consentito anche nei casi menzionati *dall'articolo 26, comma 1* della direttiva (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di **strumenti contrattuali** che offrano garanzie adeguate (*articolo 26, comma 2*).

La sentenza riguarda il trasferimento negli **USA**, dove le imprese sono tenute a **disapplicare gli accordi** di Safe Harbor se in conflitto con esigenze di sicurezza nazionale, pubblico interesse e osservanza delle leggi. Ebbene, secondo la CGUE tale possibilità lede sì il diritto al rispetto della vita privata ma la valutazione in concreto di tale incompatibilità va svolta a livello nazionale, dalle singole Autorità Garanti della Privacy, in quanto la **Commissione UE** (che nel 2000 aveva dichiarato la normativa USA adeguata e sicura) **non ha poteri vincolanti** sulle singole Autorithy.

"Qualora un'autorità nazionale o una persona ritenga che una decisione della Commissione sia invalida, tale autorità o persona deve potersi rivolgere ai giudici nazionali affinché, nel caso in cui anche questi nutrano dubbi sulla validità della decisione della Commissione, essi possano rinviare la causa dinanzi alla Corte di giustizia. Pertanto, in ultima analisi è alla Corte che spetta il compito di decidere se una decisione della Commissione è valida o no".

Ebbene, cosa cambia in concreto per le **imprese italiane**? Attualmente potrebbe non cambiare molto. Sotto il profilo della **tenuta** giuridica e vincolante degli **accordi** tra PMI italiane e paesi terzi, tutto dipende da come è stata redatta la disciplina del trattamento dati e dove gli stessi vengono trattati: i problemi sorgono infatti solo con i paesi extra-UE.

Sicuramente, per i dati trasferiti negli Stati Uniti gli accordi potrebbero essere più facilmente soggetti ad accertamenti o richieste in questo senso da parte degli interessati. La scelta migliore per le aziende che hanno rapporti a livello internazionale con paesi terzi è di redigere delle **Binding Corporate Rules** seguendo i criteri indicati a livello nazionale ed europeo, soprattutto sotto il profilo delle reciproche responsabilità e garanzie.

Ciò non toglie che, alla luce della sentenza CGUE, tutti gli **accordi** dovranno essere **rivisitati** e migliorati. Tuttavia, prima di modificare gli accordi, sarebbe opportuno per le aziende italiane attendere le linee guida o le raccomandazioni che, prevedibilmente, saranno diffuse del Garante Italiano, anche coordinandosi con le altre Autorità europee di vigilanza sulla tutela dei dati personali. Di fatto, la decisione della Corte UE (che tra

l'altro ha rinviato a quella irlandese la decisione nel merito) non ha dichiarato invalidi tutti gli accordi tra le aziende europee ed americane (o qualsivoglia paese terzo), che quindi **rimangono** pienamente **operanti**.

In realtà la sentenza sembra aver aperto **un vuoto** che la Corte non ha ritenuto di dover o poter colmare: rimandando la decisione sulla compatibilità del principio del Safe Harbor alle valutazioni delle Autorità dei singoli Stati Membri, ogni Stato potrebbe adottare decisioni diverse creando una estrema disomogeneità nel trattamento dei dati; circostanza che cozza con la tendenza e volontà (anche alla luce del nuovo regolamento sul trattamento dei dati personali) di avere una comune disciplina europea.

Protezione dati personali nel post Safe Harbor

Direttive per imprese italiane sul trasferimento dati personali negli USA dopo la sentenza sul Safe Harbor e il recepimento del Garante Privacy:

La Corte di Giustizia Europea ha stabilito che l'accordo **Safe Harbor** stipulato tra Unione Europea e Stati Uniti **non è più valido**: l'intesa consentiva la conservazione di **dati trasferiti negli USA** e appartenenti ad **utenti europei** secondo regole locali. Dunque, ogni **azienda** europea dovrà ora trovare nuove modalità per dimostrare giuridicamente che tali dati sono trattati in conformità alla legislazione UE. La sentenza non ha fatto menzione di un periodo di deroga, pertanto ha effetti immediati e di vasta portata anche per le aziende statunitensi. Comprendere le implicazioni della sentenza è infatti di cruciale importanza per le imprese che si affidano a servizi in **Cloud** erogati da data center fisicamente localizzati in territorio americano.

In **Italia** il Garante Privacy ha recepito rapidamente la sentenza con il **provvedimento del 22 ottobre**, secondo cui le imprese italiane e le multinazionali operanti nel nostro paese dovranno ricorrere alle altre possibilità previste dalla normativa sulla protezione dei dati personali per trasferire dati oltreoceano.

Linee guida

Il team legale di **NetApp** (società americana di software, sistemi e servizi per gestire e memorizzare i dati) ha messo a punto delle linee guida per aiutare le aziende a districarsi nel nuovo scenario. Sheila FitzPatrick (World Wide Data Governance & Privacy Counsel/Chief Privacy Officer) spiega che:

*«La radice del problema è la differenza fondamentale tra le **aspettative di privacy** dell'UE e la fiducia degli Stati Uniti nella crescita del mercato globale, nonostante il potenziale effetto negativo sul diritto fondamentale del cittadino di proteggere i propri dati personali. La Corte di Giustizia Europea ha evidenziato l'esistenza di soluzioni collaudate e fattibili che raggiungano gli **standard** richiesti per le aziende provider e fornitrici di **hardware** e **software**. I fornitori di soluzioni tecnologiche devono garantire la conformità dal punto di vista dello storage e dell'elaborazione dei dati e prevenire i rischi connessi ad azioni legali. I provider tecnologici non devono limitarsi alla sola fornitura infrastrutturale, ma diventare consulenti di fiducia, capendo che il rispetto della privacy dei dati va oltre la garanzia della sicurezza».*

Il Dr. Dierk Schindler (Head of Legal Field Services EMEA) sottolinea l'esigenza di correttezza delle basi tecnologiche e legali:

*«Qualsiasi azienda deve identificare e prendere **tutte le misure necessarie** per conformarsi alle leggi specifiche sulla protezione dei dati nei paesi in cui opera. Considerare la **privacy** dei dati come una questione secondaria non è più un'opzione percorribile per le aziende, ma è necessario includerla **nel go-to-market** fin dall'inizio.*

La sentenza sottolinea che programmi e pratiche efficaci sulla privacy e sulla gestione dei dati sono un dovere per tutte le organizzazioni che devono gestire dati personali. Le aziende devono rassicurare i propri clienti,

partner e dipendenti, che tutti i dati sono raccolti, elaborati, accessibili, condivisi, archiviati, trasferiti e messi in sicurezza in conformità con le leggi applicabili sulla protezione dei dati, e utilizzati solo in un modo prestabilito, legittimo e legale, indipendentemente se i dati siano archiviati presso l'azienda o presso un fornitore cloud esterno. Infatti, il successo commerciale è figlio della ***fiducia*** *che i consumatori assegnano all'azienda e qualsiasi violazione, accesso e utilizzo non autorizzato di dati personali possono rovinare qualsiasi azienda.*

*Come sempre, la sfida nasconde l'****opportunità****: la protezione dei dati implementata correttamente, crea infatti, una significativa occasione per differenziarsi rispetto alla concorrenza.»*

Operatività

Il Gruppo di Lavoro Article 29, che riunisce i garanti privacy europei, prevede come scadenza per l'emissione del nuovo Safe Harbor la fine di gennaio e ha specificato la **non validità** delle **autocertificazioni** emesse dalle imprese sulla base dei vecchi accordi. Come restare operativi senza interrompere il servizio verso i clienti o cambiare operatore e/o provider in corsa?

L'Avvocato Stefano Mele, di Carnelutti Studio Legale Associato Milano, interpellato sulle modalità di gestione del post "Safe Harbor", suggerisce una via **per non bloccare il trasferimento** dei dati personali verso gli Stati Uniti:

«Le società hanno allo stato attuale due ***soluzioni****: la prima, più pratica e veloce, si basa sulla redazione di uno* ***specifico accordo*** *per il trasferimento dei dati personali seguendo lo schema delle clausole contrattuali standard dell'Unione Europea. La seconda, un po' più macchinosa ma di carattere definitivo, è quella di redigere delle cosiddette* ***Binding Corporate Rules****, ovvero delle regole interne da applicare all'intera struttura societaria, indipendenti dal luogo dove si trovino le branch, volte a regolamentare in maniera unificata proprio il trattamento dei dati personali».*

Article 29 ricorda che Binding Corporate Rules e **Model Contract Clauses**, "possono essere usate", ma le autorità di protezione dei dati hanno pieno diritto di indagare sulla base di segnalazioni specifiche, per esercitare le loro funzioni di protezione dei diritti degli individui.

Internazionalizzazione e gestione informazioni

Come gestire a norma di legge il flusso informativo nelle imprese che intraprendono un percorso di internazionalizzazione:

Quando si affronta il tema dell'**internazionalizzazione** del business di impresa molti sono i temi che devono essere affrontati. Particolare importanza assume il tipo di **rapporto commerciale** che si intende instaurare con clienti e partner, così come i vari **vincoli** normativi nazionali ed internazionali. Il presente contributo intende concentrarsi sul sempre più importante rilievo che ha la gestione delle **informazioni** nell'ambito dell'attività imprenditoriale, ma per far ciò occorre necessariamente introdurre, sia pur in modo molto semplificato le tipologie di relazioni commerciali e le scelte contrattuali più ricorrenti.

Protezione dati

In primo luogo è importante segnalare come lo stesso **Garante Privacy** è stato sempre molto attento alla corretta gestione delle informazioni da parte delle imprese; l'Autorità infatti già da tempo ha pubblicato il **vademecum**, *"La privacy da parte dell'impresa"*. Appare evidente, infatti, come è ormai noto, che le imprese gestiscono una moltitudine di dati personali. Tanto ciò è vero che il Garante ha sottolineato come, in considerazione della struttura organizzativa (che può anche risultare molto complessa e policentrica, si pensi proprio al processo di internazionalizzazione) e degli obiettivi di business, è comunque sempre

opportuno che emerga “chi fa cosa”, “cosa e come viene fatto” e con quali scadenze. Di qui l’importanza per le imprese di una serie di **adempimenti** (le informative, il consenso dell’interessato, il controllo sull’attività lavorativa; le misure di sicurezza minime ed idonee; è molto altro ancora).

Trasferimento dati

Il vademecum del Garante affronta anche le questioni relative ai **dati personali da** “**esportare**” all’estero in relazione ai quali è necessario attenersi a precise regole. Sul punto il documento innanzitutto richiama la normativa comunitaria ai sensi della quale i dati personali possono circolare liberamente entro l’Unione Europea, chiarendo invece, che per trasferire dati al di fuori dell’Unione Europea devono essere garantiti standard di protezione adeguati a quelli europei: in caso contrario è vietato trasferire dati personali. Ai fini di una semplificazione delle relative procedure il Garante pubblica sul proprio sito internet un elenco aggiornato degli Stati “terzi” (cioè non appartenenti all’Unione europea o allo Spazio Economico Europeo) che sono già ritenuti affidabili a livello europeo e per i quali non è necessaria alcuna autorizzazione specifica per il trasferimento. Nel caso invece di imprese che devono **trasferire dati verso Paesi terzi** (non inseriti nella lista), anche se soltanto all’interno della propria struttura societaria (per esempio proprio nel caso in cui si stia attuando un piano di sviluppo di internazionalizzazione), è necessario che vengano adottate adeguate **norme vincolanti d’impresa** (BCR – Binding Corporate Rules) che devono essere autorizzate dalle Autorità Europee di protezione dati come, appunto, il Garante italiano. In alcuni casi potrebbe anche essere sufficiente redigere un c.d. “contratto di trasferimento” le cui clausole sono comunque riconducibili a quelle che si analizzeranno qui di seguito in relazione alle BCR.

Deve anche essere precisato che la normativa sul trattamento dei dati personali prevede alcune **eccezioni** al divieto di trasferire dati in Paesi terzi: è consentito, ad esempio, il trasferimento se vi è l’apposito consenso dell’interessato (consenso scritto nel caso in cui si tratti di dati sensibili), oppure quando il trasferimento risulta necessario per l’esecuzione di obblighi derivanti da un contratto del quale è parte l’interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell’interessato. Se questa, in linea generale è la disciplina cui devono far riferimento le imprese che intendono aprirsi ai nuovi mercati internazionali, è importante capire, di fatto, quali effettive prescrizioni queste devono adottare.

Vincoli

A questo punto sembra opportuno richiamare quali siano comunemente le **scelte** che le imprese adottano quando decidono di intraprendere la strada dell’internazionalizzazione. Questo perché a seconda della scelta che si intende fare i **vincoli** possono essere più o meno stringenti.

- Alcune imprese preferiscono creare all’interno della propria struttura una **divisione** specificamente organizzata per interagire con i nuovi mercati soprattutto sotto il profilo del marketing sviluppando pertanto questo settore ricorrendo alle opportunità offerte dall’e-commerce.
- Una ulteriore possibilità, tipica per le imprese di grandi dimensioni, è quella che privilegia invece la c.d. **delocalizzazione**; in questo caso ci sono indubbi vantaggi sotto molteplici profili, sia per quanto concerne il rapporto diretto con il mercato di riferimento.
- Ultima ipotesi, probabilmente la più facile da seguire dalle PMI è anche quella di agganciarsi a un soggetto imprenditoriale già operante nel mercato di riferimento e che funzioni come **ponte** verso il nuovo mercato.

In tutte tre le ipotesi, ma in particolare per le ultime due, dovrà prestarsi particolare attenzione ai **contratti** che si andranno a redigere, sia quelli aventi ad oggetto la compravendita dei beni o servizi offerti dall’impresa, sia quelli che formalizzano i rapporti con le realtà esistenti nel Paese verso cui ci si vuole espandere. Sul punto, in via generale, appare sicuramente consigliabile ai fini della redazione dei contratti ricorre ai **Principi UNIDROIT**, in materia di contratti commerciali; in ogni caso dovrà comunque tenersi in

debito conto se il processo di internazionalizzazione coinvolge Paesi extracomunitari legati all'Italia da convenzioni e accordi bilaterali anche parziali, ovvero Paesi extracomunitari non convenzionati.

Gestione dati personali

A questo punto è possibile approfondire la tematica inerente alla **gestione dei flussi informativi** in relazione alla quale ci sono stati interventi normativi del Garante. Come già accennato, la normativa europea, in particolare la direttiva 95/46/CE stabilisce che i dati personali possono essere trasferiti in un Paese non appartenente all'Unione Europea qualora il Paese terzo garantisca un livello di protezione adeguato.

Su questa base il **Gruppo ex Articolo 29** ha ritenuto che le BCR potessero costituire uno strumento di trasferimento dei dati personali verso Paesi terzi astrattamente idoneo ad assicurare un livello adeguato di protezione dei diritti degli interessati e dunque compatibile con la disciplina contenuta nella direttiva 95/46/CE. A tal fine ha adottato tutta una serie di **provvedimenti** che indicano i specifici requisiti e clausole che le imprese devono adottare nella redazione delle BCR: WP 74 del 3 giugno 2003, WP 107 del 14 aprile 2005, WP 108 del 14 aprile 2005, WP 153 , WP 154, WP 155 del 24 giugno 2008 e WP 195 del 6 giugno 2012 contenente un nuovo modello di norme vincolanti d'impresa definito "BCR for processor" (cioè il responsabile del trattamento).

Sulla questione è intervenuta anche la **Commissione europea** la quale ha adottato alcune decisioni contenenti altrettanti set di **clausole** tra cui quelle:

- per il trasferimento dei dati da un titolare stabilito nel territorio europeo ad un altro titolare stabilito in un Paese extra-UE (decisioni 2001/497/CE e 2004/915/CE);
- per il trasferimento dei dati da un titolare stabilito nel territorio europeo ad un responsabile stabilito in un Paese extra-UE (decisione 2010/87/UE, che introduce nuove definizioni: "esportatore" è il titolare che trasferisce i dati personali e "importatore" è il responsabile o il titolare stabilito nel Paese terzo che riceve i dati).

Nell'ambito della **normativa italiana** invece occorre richiamare l'art. 44, comma 1, lett. a), del **Codice Privacy** nel quale si trova conferma che il **trasferimento di dati personali** diretto verso un Paese non appartenente all'Unione Europea è consentito quando è **autorizzato** dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, individuate dall'Autorità anche in relazione a **regole di condotta** esistenti nell'ambito di società appartenenti a un medesimo gruppo e denominate *Binding Corporate Rules*. In questo modo l'interessato viene garantito sia dal punto di vista normativo potendo applicare le prescrizioni del Codice, sia dal punto di vista privatistico facendo valere nei confronti dell'impresa le Bcr; Tanto è vero, si ritiene, che sotto il profilo strettamente giuridico l'adozione di dette regole di condotta costituiscono un fatto astrattamente idoneo a produrre effetti giuridicamente vincolanti nell'ordinamento giuridico italiano, ai sensi dell'art. 1173 cod. civ.

La **redazione delle BCR**, quindi, è il passaggio fondamentale per gestire in maniera corretta il flusso informativo che si viene a creare per le imprese che decidono di intraprendere il percorso di internazionalizzazione.

Internazionalizzazione: il trasferimento dei dati personali

Linee guida il corretto trattamento e trasferimento di dati personali nell'ambito di operazione commerciali con paesi esteri:

Dall'analisi dei provvedimenti del Garante Privacy è possibile individuare gli elementi fondanti per la costruzione di efficaci **BCR** (*Binding Corporate Rules*) da adottare per il **trasferimento** di **informazioni**

personali nell'ambito di attività di **internazionalizzazione** d'impresa, tali da passare indenni al vaglio autorizzativo dell'Autorità.

In primo luogo è importante il dato definitorio. La ragione è chiara: nel momento in cui si ragiona in termini di internazionalizzazione, le BCR devono essere conosciute e conoscibili da tutti gli interessati, ne consegue che le norme vincolanti dovranno essere redatte, per forza di cose, quanto meno in **due lingue**. Tale esigenza pone il problema di ricorrere a termini interpretabili in un solo senso anche in lingue diverse. Dalla lettura dei provvedimenti emessi dal Garante si evince infatti che sono emerse questioni relative – per esempio, ma non solo – alle **definizioni** di titolare del trattamento, responsabile del trattamento ed incaricato alle misure idonee di sicurezza. Un secondo elemento fondamentale attiene all'individuazione dei soggetti i cui **dati personali** verranno trasferiti intra-gruppo verso Paesi terzi e che devono essere **esattamente individuati** ai fini del pieno rispetto dei principi di proporzionalità e necessità dettati dal Codice della Privacy. Gli **interessati** possono essere: dipendenti (anche "ex"), c.d. "persone a carico", clientela, fornitori, candidati all'assunzione, tirocinanti, utenti dei siti web, gli azionisti, partner commerciali.

Trattamento

Di pari importanza assume l'esatta individuazione (nel rispetto dei principi appena richiamati) delle **finalità del trattamento**, per le quali si richiede l'autorizzazione al trasferimento. A titolo di esempio si possono individuare: gestione delle risorse umane, adempimenti contabili e amministrativi, attività di customer, management e marketing, gestione del rapporto di lavoro, gestione dei piani di offerta azionaria, sviluppo aziendale e creazione e gestione delle relazioni esterne, infrastruttura e supporto tecnologico, gestione dei mezzi e dei viaggi, conoscenze. Come è facile intuire, la **mole di informazioni** da gestire e regolare durante e a fine processo di internazionalizzazione è veramente notevole.

Responsabilità

Un punto ulteriore su cui sia la normativa europea sia il Garante italiano si soffermano è la previsione della cosiddetta **clausola di responsabilità** secondo la quale l'interessato, in qualità di terzo beneficiario, può far valere nei confronti dell'impresa i **vincoli** previsti dalle **BCR** innanzi alle Autorità di protezione dei dati personali e alle Autorità Giudiziarie competenti (si ricordi il richiamo sopra accennato all'art.1173 c.c.), anche sotto il profilo del **risarcimento** del danno. Sotto questo profilo alcune aziende si sono preoccupate, a maggior tutela dell'interessato, anche di prevedere nell'ambito delle proprie BCR un collegamento tra clausola di responsabilità e criteri di scelta in materia di **giurisdizione** avanti alla quale è possibile ricorrere per far valere i propri diritti.

Privacy

Per sottolineare l'importanza e l'effettivo valore precettivo delle BCR nell'impresa, è consigliabile prevedere nelle norme vincolanti un esplicito richiamo alla **privacy policy** aziendale o quanto meno ai principi in materia di protezione dei dati personali con particolare riferimento a: diritto di accesso ai dati personali e altri diritti, modalità del trattamento e requisiti dei dati, informativa, diritto di ottenere il blocco o la cancellazione dei dati, trattamento dei dati sensibili e di quelli a carattere giudiziario, misure di sicurezza. Insomma è fondamentale che l'impresa formalizzi la propria **conformità** alle prescrizioni dettate dal **d.lgs. 196/03**.

Trasparenza

Un'ultima considerazione: in ragione del rilevante valore che assumono ai fini del corretto trattamento dei dati personali trasferiti infra-gruppo verso un Paese terzo, le BCR devono essere portate **a conoscenza** di tutti i soggetti interessati, in linea con i criteri di consapevolezza, trasparenza e consenso informato che caratterizzano la normativa in tema di privacy. Proprio per tale ragione il Garante ritiene che le **BCR**, come la privacy policy alle stesse collegate, dovranno essere **pubblicate** su **Internet** nel caso della clientela e nell'**Intranet aziendale** con riguardo ai dipendenti.

Conformità

In chiusura va poi rilevato come il Garante precisi che le **operazioni** di trattamento dei dati personali, anche se poste in essere a seguito del rilascio dell'autorizzazione, saranno lecite solo ove **conformi alla normativa nazionale** vigente e alle sue successive modificazioni, nonché alle specifiche disposizioni in materia di protezione dei dati personali, con particolare riferimento ai presupposti di legittimità delle attività di **raccolta dei dati** oggetto del trasferimento e alla sussistenza dei presupposti di legittimità per la **comunicazione** dei dati medesimi.

Non solo: il Garante precisa altresì che ai sensi dell'art. 154, comma 1, lett. a) e d) del Codice, lo stesso ha il compito di controllare la conformità dei trattamenti di dati alla disciplina applicabile e può, anche d'ufficio, vietare o disporre il blocco, nonché adottare gli ulteriori provvedimenti previsti dalla medesima; si riserva di svolgere **in qualsiasi momento** i necessari **controlli** sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché di adottare, se necessario, i provvedimenti previsti dal Codice.

Per quanto scontato sia, va rilevato che ai sensi dell'art. 157 del Codice, l'impresa dovrà comunicare al Garante entro novanta giorni dall'approvazione di eventuali modifiche di carattere sostanziale apportate al testo delle BCR.

Privacy UE, le nuove regole Marketing

Le nuove direttive UE sul trattamento dei dati personali impattano sulle attività di Marketing: cambiano informativa e diritti.*

Il nuovo **Regolamento UE** sulla protezione dei **dati personali** è entrato in vigore il 25 maggio 2018. La normativa interessa molteplici aspetti delle normali **attività aziendali**. In primis sicurezza e **privacy** delle informazioni e controllo dei lavoratori, ma anche politiche di **marketing**, in particolare quello diretto e **digitale**. Più volte il Garante è intervenuto su questo tema, tanto che nel vademecum del febbraio 2015 si legge:

"Il rispetto del consumatore e il corretto uso dei suoi dati personali – a partire da quelli necessari per contattarlo fino alle informazioni più private, come gusti e preferenze – differenziano le imprese che vedono i propri clienti come semplice preda, da quelle che scelgono di operare in modo trasparente, ponendo al centro della loro attività sia la qualità dei propri prodotti e servizi sia la fiducia dei propri acquirenti."

Il **vademecum** rimane valido e attuale, tuttavia si attendono aggiornamenti alla luce del nuovo Regolamento. Nello svolgere (direttamente o per conto terzi) attività di marketing, per l'azienda permangono i **principi** fondamentali indicati dall'Autorità:

- il consumatore deve essere sempre informato del trattamento dei dati personali;
- per utilizzare i dati personali di un individuo (recapiti, abitudini di consumo…) per qualunque altra finalità serve il consenso;
- nel trattamento dei dati devono essere sempre rispettati i principi di finalità, proporzionalità e non eccedenza, ossia lo scopo originario per il quale i dati sono stati raccolti e usati.

Quindi, l'**informativa** – che il Regolamento impone sia scritta in modo semplice (art. 7 GDPR) – e il **consenso** – che la nuova disciplina sulla privacy dispone sia inequivocabile – nella loro veste rafforzata dal Regolamento rimangono i cardini intorno o a cui devono svilupparsi le attività di marketing. Il Regolamento ha infatti reso più incisivi questi aspetti; ne consegue che le aziende sono chiamate ad intervenire con non pochi "**aggiustamenti**".

Una interessante **novità** è l'introduzione del principio dell'**interesse legittimo** al trattamento dei dati personali. Il Regolamento chiarisce infatti che: *"può essere considerato legittimo interesse trattare dati personali per finalità di marketing".*

L'impresa dovrà pertanto compiere adeguate **valutazioni** al fine di giustificare il proprio interesse legittimo (*Considerando 47*). Infatti, i legittimi interessi di un titolare possono giustificare un corretto trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative di quest'ultimo.

Insomma, nell'acquisire il consenso al **trattamento dei dati** per attività di marketing, l'impresa dovrà fornire un'informativa che non lasci spazio ad alcun equivoco, poiché in caso contrario gli interessi e i diritti dell'interessato andranno a prevalere su quelli legittimi del titolare, rendendo non corretto il trattamento.

Inoltre, anche qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato deve avere il diritto, in qualsiasi momento e gratuitamente, di opporsi al trattamento iniziale o ulteriore, compresa la **profilazione** connessa al marketing diretto.

Quindi, da quanto riportato sino ad ora, la regola vigente in materia di marketing sarà quella dell'**opt-out**: non il consenso a ricevere comunicazioni commerciali bensì il diritto a sottrarsene; sulla base giuridica di un giustificato interesse legittimo sarà possibile svolgere attività di marketing, comunicando esplicitamente e chiaramente all'interessato il diritto di opporvisi (art. 21 GDPR).

L'operazione che giustifica questa nuova normativa è sin troppo chiara: l'UE ha inteso dare più tutele al consumatore ma anche ampliare gli spazi di manovra delle aziende nell'organizzare e sviluppare le proprie attività di business.

Pubblicità diretta: telefono, email, posta ordinaria

Telemarketing e Direct Marketing: dal Testo Unico per la Privacy al Registro Opposizioni, analisi della norma e delle regole vigenti in materia di comunicazioni commerciali dirette.

In pochi mesi la regolamentazione in materia di comunicazioni commerciali, telefoniche e non solo, è radicalmente mutata (in vigore da febbraio 2011) per via del DPR n.178/2010 e del Provvedimento del Garante Privacy n.16/2011, che in un certo senso hanno invertito il principio fondamentale prima utilizzato.

Telemarketing: regole per utenti

In passato, l'azienda di Telemarketing e le società di call center dovevano disporre del **consenso preventivo** da parte dei destinatari prima di sottoporre proposte commerciali (opt-in), mentre dal primo febbraio 2011 le imprese possono godere del **silenzio-assenso** senza alcun consenso preventivo (opt-out), purché i destinatari, persone fisiche e giuridiche, non abbiano **comunicato il dissenso** esplicito previa **registrazione al Registro delle opposizioni**, riservato agli utenti iscritti in elenchi telefonici pubblici.

C'è un ulteriore però: agli iscritti al **Registro Opposizioni** non è consentito rivolgere attività di Telemarketing, purché essi stessi non abbiano in altre circostanze fornito il consenso (spesso obbligatorio quando si sottoscrive un servizio, per esempio) alle proposte. Se infatti il destinatario è iscritto nel Registro, ma in passato ha autorizzato in forma scritta e quindi documentabile una singola l'impresa a contattarlo, tale impresa può inviargli informazioni.

Per questo motivo, per "chiamarsi fuori" gli utenti devono espressamente comunicare ad ogni impresa, attraverso qualsiasi forma di comunicazione, di non voler ricevere informazioni commerciali: gli utenti possono **in qualsiasi momento ritirare l'autorizzazione**.

In via generale, dunque, la nuova regolamentazione consente che i recapiti telefonici inseriti in elenchi quali albi professionali, registri pubblici o altri elenchi a cui chiunque possa attingere possano essere utilizzarti, anche senza consenso, per attività di comunicazione telefonica a fini promozionali o promozione riconducibile all'attività del destinatario (diritto che decade in caso di espressa opposizione).

Regole per aziende di Telemarketing

L'**azienda** che intende svolgere attività di Telemarketing deve anch'essa **iscriversi al Registro** delle Opposizioni, rendendo noti i numeri telefonici che intende contattare (in modo che il sistema possa escludere quelli degli utenti che si iscrivono al Registro, con costi a carico dell'azienda che ne fa richiesta). Una volta ottenuta la **lista dei non-iscritti** si può partire con le comunicazioni commerciali, purché ad ogni destinatario vengano forniti tutti i dati del caso:

- nome azienda
- elenco da cui sono stati presi i recapiti
- indicazioni per l'iscrizione al Registro qualora non si vogliano più ricevere informazioni pubblicitarie.

Responsabilità

La **responsabilità dell'impresa** non si riduce se il servizio è svolto in outsourcing: l'azienda esterna non sempre diventa direttamente responsabile rispetto a **irregolarità** o violazioni della privacy.

Può accadere ad esempio che al momento del contatto la ditta esterna si spacci per l'azienda che commissiona il telemarketing, o che imprecisioni del contratto che intercorre tra le due imprese finiscano per scaricare le responsabilità su quella che esternalizza. In questo caso le irregolarità vengono addebitate ad **entrambe le imprese**, ma il committente potrà rivalersi sulla ditta esterna in base alle clausole del contratto, in cui è necessario stabilire preventivamente l'obbligo di effettuare l'attività di promozione in ottemperanza agli obblighi che individuano la sfera privata dei destinatari.

-- fine del documento --