Regolamento generale sulla protezione dei dati (GDPR)

La guida rapida di Sage per le aziende

Sommario

Introduzione 3

Infografica: GDPR a colpo d'occhio 4

Le basi 5

Il GDPR in breve 5

- Diritti individuali: descrizione e informativa al pubblico 5
- Consenso 5
- Diritto allo spostamento e al trasferimento dei dati personali (portabilità dei dati) 6
- Ambito di applicazione allargato 6
- Prova di conformità 6
- Privacy dalla «a» alla «z» 6
- Denuncia obbligatoria delle violazioni 7
- Responsabile per la protezione dei dati (DPO) 7
- Sanzioni 7

Brexit 7

GDPR: principi fondamentali 8

- Principi di protezione dei dati 8
- Legittimità del trattamento 8
- Trasferimento internazionale dei dati 8

Cosa potete fare subito 8

Dichiarazione di non responsabilità di Sage 9

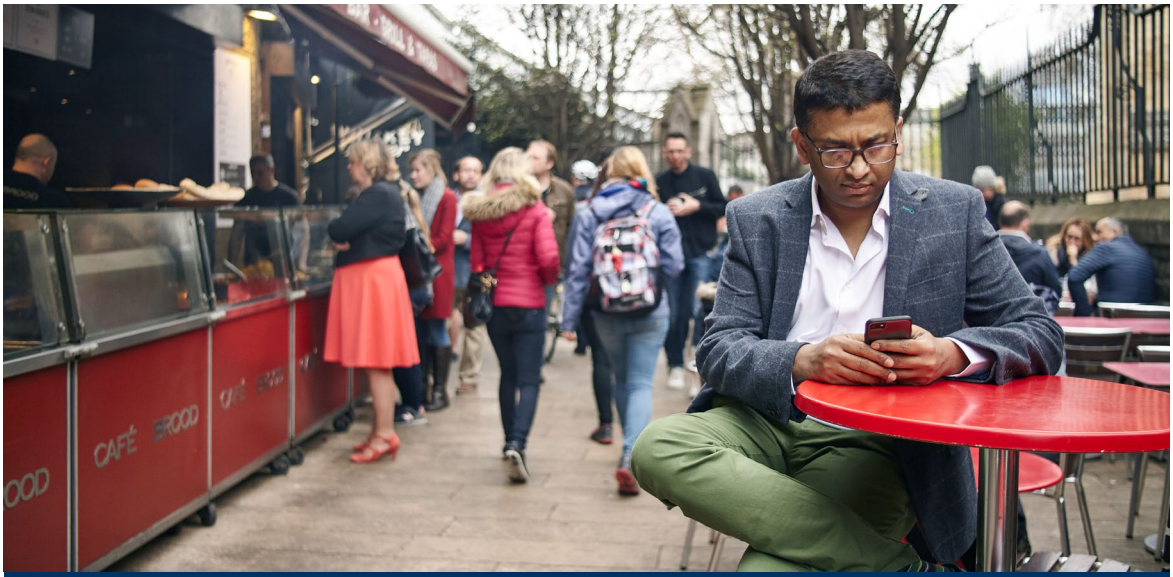
Introduzione

Il Regolamento generale sulla protezione dei dati («GDPR») è il nuovo inquadramento normativo che entrerà in vigore il 25 marzo 2018 nell'Unione Europea («UE»). Dato che i Regolamenti europei hanno un effetto diretto su tutti gli Stati membri, il GDPR avrà la precedenza su qualsiasi altra normativa nazionale.

L'obiettivo del GDPR è la protezione dei dati personali, ad esempio dei dati riguardanti i singoli individui. Di fatto, il GDPR è una delle più grandi rivoluzioni in materia di trattamento dei dati personali che riguarderà non solo le aziende ma anche singoli individui, enti, autorità pubbliche, agenzie e altri organismi che trattano i dati personali di persone residenti nell'UE. Il GDPR si estende anche a fornitori e altre eventuali terze parti addette al trattamento dei dati personali per conto di un'azienda.

Il GDPR ha una portata sorprendentemente vasta, abbracciando tutti gli Stati Membri dell'Unione Europea, compreso il Regno Unito post-Brexit nel 2019, che lo incorporerà anche nella giurisprudenza britannica. Al contrario della Direttiva europea 95/46 sulla protezione dei dati personali, il GDPR si applica anche a tutte le aziende non europee che offrono beni o servizi a persone residenti nell'UE o che ne monitorino il comportamento all'interno dell'UE. Ad esempio, saranno coinvolte tutte le aziende americane di alloggiamento di siti web accessibili da persone residenti nell'UE.

Il GDPR avrà effetti enormi sui molti reparti di tante aziende in tutto il mondo. Ad esempio, alcune aziende potrebbero anche dover assumere o incaricare un Responsabile per la protezione dei dati. Quasi tutte dovranno mettere in pratica procedure e dispositivi di sicurezza aggiuntivi. È consigliabile far eseguire un controllo da parte di un esperto del settore e, vista la possibilità di incorrere in sanzioni fino al 4% del fatturato globale annuo o pari a 20 milioni di euro, delle due la cifra più alta, la conoscenza del GDPR deve essere considerata obbligatoria.



Il presente documento è da intendersi come una guida concisa e semplificata per le aziende. È possibile reperire ulteriori informazioni rivolgendosi alle autorità competenti, come l'Information Commissioner's Office (ICO) nel Regno Unito con il suo documento «Overview of the General Data Protection Regulation». Vi preghiamo di leggere la dichiarazione di non responsabilità di Sage riportata alla fine di questa guida.

Infografica:

GDPR a colpo d'occhio

Regolamento generale sulla protezione dei dati (GDPR)

Consenso

Deve essere confermato da una dichiarazione o altra affermazione chiara. Non è possibile presumere il consenso né usare caselle pre-barrate sui siti web.

Diritti individuali

Amplia notevolmente i diritti dei singoli cittadini e le informazioni che sono tenuti a ricevere circa le attività di trattamento dei dati.

Sanzioni

Possono arrivare al 4% del fatturato globale annuo o 20 milioni di euro, delle due la cifra più alta. Non è necessario che si verifichi una perdita di dati per incorrere in sanzioni.

Portabilità dei dati

I singoli cittadini ora hanno il diritto di spostare, copiare o trasferire i propri dati personali, anche alla concorrenza.

Denuncia obbligatoria delle violazioni

Gli addetti al controllo dati personali sono tenuti ad avvisare le autorità competenti, come l'ICO nel Regno Unito, entro 72 ore dalla constatazione della violazione. Le persone interessate devono essere informate in caso di violazioni gravi.

Responsabile per la protezione dei dati

Può essere obbligatorio. Deve essere un esperto delle leggi in materia di protezione dei dati. Può essere un dipendente o impiegato a progetto.

Privacy dalla «a» alla «z»

Considerazioni sulla privacy devono essere incorporate in tutti i processi aziendali e solo i dati strettamente necessari possono essere utilizzati.

Ambito di applicazione allargato

Riguarda la vostra azienda e tutti gli addetti al trattamento dei dati per vostro conto, anche al di fuori dell'UE.

Le basi

Il GDPR stabilisce i requisiti minimi per il trattamento di tutti i dati personali. Si definiscono «dati personali» tutti i dati relativi specificamente a un individuo e che lo identificano (compresi dettagli come aspetto fisico e parametri biometrici).

La maggior parte delle aziende raccoglie dati personali fin dal primo contatto con un individuo, a volte addirittura senza rendersene conto. Ad esempio, può essere considerata raccolta di dati personali un'azione elementare come l'utilizzo di cookie per il monitoraggio dei siti web che identificano un utente del vostro sito. Il concetto di raccolta si estende poi a procedimenti molto più dettagliati come la registrazione di un individuo in un database di gestione delle relazioni con i clienti («CRM»), e molto altro. Anche il caso in cui i dati personali vengano raccolti o trattati a beneficio esclusivo dell'individuo stesso ricade nelle competenze del GDPR.

Così come la Direttiva UE 95/46, il GDPR ribadisce tre serie fondamentali di regole relative ai dati personali: principi di protezione dei dati, legittimità del trattamento e restrizioni sui trasferimenti internazionali. La maggior parte delle aziende e molte persone dovrebbero già essere a conoscenza delle suddette regole. Le tre sopracitate serie di regole sono descritte nel dettaglio in questo documento di cui è vivamente consigliata la lettura, anche solo per rinfrescare delle conoscenze già esistenti.

In ogni caso, il GDPR introduce molte nuove regole importanti.

Il GDPR in breve

Ecco in breve le aree principali del GDPR, con particolare riferimento alla Direttiva UE 95/46 sulla protezione dei dati.

Diritti individuali e l'obbligo d'informazione verso gli individui

L'attuale legislazione UE in materia di protezione dei dati (Direttiva 95/46) sancisce i diritti dei singoli individui sui propri dati personali e descrive nel dettaglio le informazioni che le aziende sono tenute a fornire agli stessi, comprese le informazioni circa le modalità e gli scopi di utilizzo dei loro dati personali. In molti casi, tali informazioni prendono la forma di notifiche o informative sulla privacy su un sito web.

Il GDPR amplia notevolmente quest'ambito, sancendo ulteriori diritti che devono, ancora una volta, essere comunicati ai singoli individui. In particolare, i singoli individui devono essere informati dei seguenti diritti (a titolo non esaustivo):

1. di reclamare rivolgendosi alle autorità preposte, come l'ICO nel Regno Unito;
2. di ritirare il consenso al trattamento dei propri dati personali (vedi sotto);
3. di accedere ai propri dati personali e farli correggere o cancellare («diritto a essere dimenticati») dall'azienda ed eventuali terze parti che ne abbiano preso visione;
4. di essere informati dell'esistenza di eventuali procedimenti automatici di trattamento dei dati personali (inclusa la creazione di profili);
5. di opporsi a determinate tipologie di trattamento dati, es. pratiche di direct marketing e decisioni basate esclusivamente sul trattamento automatico dei dati;
6. di essere informati sulla durata del periodo di conservazione dei propri dati personali;
7. di ricevere i dati relativi al Responsabile per la protezione dei dati (vedi sotto).

Inoltre, ciascun individuo ha il diritto di chiedere a organizzazioni no-profit di esercitare diritti e promuovere azioni a proprio nome, similmente a ciò che avviene negli Stati Uniti con le class action.

Consenso

Se la vostra azienda raccoglie dati sulla base del consenso espresso dai singoli individui, dovete sapere che, con il GDPR, il suddetto consenso deve ora essere confermato da una dichiarazione o altra affermazione chiara, mentre la legislazione UE sulla protezione dei dati ha sempre richiesto che il consenso fosse libero. In altre parole, d'ora in avanti non costituiranno più espressione di consenso le caselle pre-barrate sui siti web o il silenzio/l'inattività del singolo individuo dopo aver preso visione di un'informativa sulla privacy.

Inoltre, il consenso non può più essere universale, per cui le aziende non potranno utilizzare il consenso espresso da una persona in un dato momento durante il rapporto commerciale come consenso per altri tipi di trattamento dei dati personali. Sono richiesti consensi distinti per le diverse operazioni di trattamento dei dati personali.

Infine, i singoli individui dovranno essere informati del diritto di ritirare il proprio consenso in qualsiasi momento, e le modalità di ritiro del consenso dovranno essere semplici quanto quelle di concessione dello stesso.

I consensi già accordati dai singoli individui dovranno essere rivisti per assicurarne l'adeguamento ai requisiti del GDPR. Nel caso di conflitti o ambiguità le aziende dovranno stabilire nuove basi legali per il trattamento dei dati (es. ove questo sia necessario per l'esecuzione di un contratto), ottenere un nuovo consenso, oppure cessare il trattamento dei dati personali in questione.

Diritto allo spostamento e al trasferimento dei dati personali (portabilità dei dati)

I singoli individui ora hanno il diritto di spostare, copiare o trasferire i propri dati personali da un posto all'altro, inclusa la concorrenza. Esempio: una piattaforma musicale genera una playlist per un utente; quando questo passa a un diverso fornitore di servizi ha il diritto di portarla con sé. Il formato dei dati personali deve essere inoltre strutturato, di uso comune e leggibile dalle macchine in modo da poter essere utilizzato e condiviso facilmente.

La regola di rendere i dati perfettamente portabili e facili da utilizzare da terze parti comporterà, verosimilmente, notevoli adeguamenti in campo informatico con relativi costi.

Ambito di applicazione allargato

In parole semplici, in base al GDPR non saranno più solo le aziende che raccolgono i dati personali a essere responsabili per eventuali violazioni alla normativa vigente, ma anche eventuali terze parti addette al trattamento dei suddetti dati per conto delle aziende, siano esse un'altra azienda, un'organizzazione o un singolo individuo. In ogni caso, questo non significa che un'azienda può semplicemente passare i dati personali raccolti a una terza parte per poi lavarsene le mani. L'azienda originaria deve assicurarsi, infatti, che eventuali terze parti coinvolte agiscano nel rispetto del GDPR.

In aggiunta, l'ambito geografico potenziale del GDPR si estende ben oltre l'UE, andando a toccare qualsiasi azienda (o terza parte addetta al trattamento dei dati personali per conto di quest'ultima) che offra beni o servizi a persone residenti nell'UE o che monitori il comportamento di persone all'interno dell'UE. Nello specifico, non è necessario che i beni o i servizi proposti richiedano un pagamento, per cui anche enti di beneficenza e organizzazioni non governative sono soggette al GDPR.

Dato che l'UE è un partner commerciale per molti Paesi, un ambito di applicazione più ampio del GDPR si traduce in un impatto sulla maggior parte delle aziende in tutto il mondo, e richiederà che queste ultime si conformino a esso se vogliono operare all'interno di Stati membri dell'UE, sia in maniera diretta che in qualità di terze parti per conto di altri.

Prova di conformità

Attenersi al GDPR non è sufficiente. Un'azienda deve provare la propria conformità in base al requisito del GDPR che riguarda la «responsabilità», e questo significa rispettare requisiti piuttosto onerosi circa la tenuta dei registri. In particolare, dovranno essere conservati i dati relativi alla documentazione delle attività di trattamento*, richieste di accesso ai dati, violazioni, modalità di ottenimento del consenso e valutazioni d'impatto sulla protezione dei dati personali (vedi sotto).

Questa regola, ancora una volta, riguarda le terze parti addette al trattamento dei dati personali per conto delle aziende, sebbene i requisiti non siano così dettagliati.

** Valido per le aziende con più di 250 impiegati, o quelle con meno impiegati ma in cui il trattamento dei dati costituisca un rischio per i diritti e le libertà dei singoli cittadini, non sia occasionale o includa dati appartenenti a categorie speciali, come informazioni su salute, religione o orientamento sessuale.*

Privacy dalla «a» alla «z»

Dovranno essere istituite misure tecniche e organizzative per tutta la durata della conservazione dei dati personali che soddisfino le aspettative in materia di privacy dei singoli cittadini, dal principio dell'attività in questione, per tutta la sua durata e fino alla sua cessazione. Questo aspetto è chiamato «Privacy by Design», che vuol dire incorporare considerazioni sulla privacy nella stessa progettazione di qualsiasi processo aziendale.

Per di più, dovranno essere trattati esclusivamente i dati personali strettamente necessari allo scopo, concetto descritto con la definizione di «minimizzazione dei dati» o «Privacy by Default».

In realtà, l'implementazione dei concetti di Privacy by Design e Privacy by Default comporterà la necessità di formazione continua del personale e di controlli regolari, minimizzazione dei dati raccolti, accesso ristretto ai dati personali in base alle reali necessità e attuazione di misure di sicurezza tecniche e organizzative adeguate come uso di pseudonimi e criptaggio.

Denuncia obbligatoria delle violazioni

In caso di violazione del GDPR, le aziende che raccolgono dati personali sono tenute ad avvisare le autorità competenti, come l'ICO nel Regno Unito, entro 72 ore dalla constatazione della violazione. Le terze parti addette al trattamento dei dati personali per conto delle aziende in questione dovranno immediatamente avvisare le stesse.

Nel caso in cui la violazione rappresenti un grave rischio per la persona in questione, le aziende saranno tenute ad avvisarla immediatamente.

Responsabile per la protezione dei dati (DPO)

In base al GDPR, le aziende e tutte le eventuali terze parti addette al trattamento dei dati personali per loro conto dovranno designare un Responsabile per la protezione dei dati («DPO») se: (i) sono un ente pubblico; (ii) l'attività principale dell'azienda o della terza parte comporta il monitoraggio di persone su larga scala; o le attività principali consistono nel trattamento su larga scala di dati personali di categoria speciale, compresi i dati relativi a reati e condanne penali. Il DPO deve essere un esperto di leggi in materia di protezione dei dati. Non è necessario che il DPO sia un dipendente dell'azienda per la quale può essere impiegato solo a progetto per lo svolgimento del ruolo specifico in questione. I dati relativi al DPO dovranno essere comunicati all'autorità competente, come l'ICO nel Regno Unito.

Sanzioni

Le sanzioni per la mancata ottemperanza al GDPR sono severe e possono arrivare al 4% del fatturato globale annuo dell'azienda o a 20 milioni di euro, delle due la cifra più alta. Non è necessario che si verifichi una perdita di dati per incorrere in sanzioni. Si prega di notare che non sono previste eccezioni o esclusioni per le piccole aziende. Inoltre, è possibile per i singoli cittadini promuovere una causa di class action con la richiesta di un'indagine governativa formale nel caso in cui un'azienda non rispetti il GDPR.

Brexit

In seguito alle votazioni del 2017, il Regno Unito ha assegnato il mandato di cinque anni a un governo conservatore. Durante tale mandato, e più precisamente nel 2019, il Regno Unito lascerà l'Unione europea. Così come per tutti gli Stati membri dell'UE, il GDPR avrà valore anche per il Regno Unito fino ad allora. Comunque, nell'annuncio della nuova legislazione dopo le elezioni, in materia di leggi sulla protezione dei dati è stato dichiarato quanto segue:

> *«... applicheremo il Regolamento generale sulla protezione dei dati e la nuova Direttiva relativa al trattamento dei dati delle forze dell'ordine, tenendo fede ai nostri impegni mentre saremo ancora uno Stato membro dell'UE e permettendo al Regno Unito di restare in una posizione privilegiata per il mantenimento della capacità di condividere dati con altri Stati membri dell'UE e a livello internazionale dopo la nostra uscita dall'UE.»*
>
> *Fonte: Discorso della regina Elisabetta II, giugno 2017*

Pertanto è possibile, ma non certo, che il Regno Unito dopo la Brexit sarà considerato dalla Commissione europea un Paese che fornisce protezione «adeguata» e che, dunque, non incorrerà in potenziali problemi legati alla protezione dei dati con conseguenti divieti di trasferimento. Tornate a trovarci per ulteriori informazioni sulle decisioni future.

La nuova legislazione britannica sostituisce il Data Protection Act del 1998, che si basava sulla Direttiva UE 95/46.

GDPR: principi fondamentali

Oltre ai nuovi requisiti illustrati in precedenza, e come per la Direttiva UE 95/46, il GDPR ribadisce tre serie fondamentali di regole relative ai dati personali. In parole semplici, possono essere riassunte come segue.

- ***Principi di protezione dei dati:*** i dati personali devono essere trattati nel rispetto delle leggi e in maniera equa e trasparente per la persona interessata. I dati devono essere raccolti per fini specifici, espliciti e legittimi e non possono essere ulteriormente utilizzati in maniera incompatibile con questi principi. I dati personali raccolti devono essere adeguati, pertinenti e limitati al necessario. I dati raccolti devono essere accurati e aggiornati, e deve essere fatto tutto il possibile per assicurare che i dati inaccurati vengano cancellati o corretti immediatamente. I dati devono essere conservati in maniera da identificare la persona cui appartengono solo per il tempo strettamente necessario e devono essere trattati in modo da assicurarne l'adeguata sicurezza anche contro perdite, distruzione, danneggiamento o accesso illecito.
- ***Legittimità del trattamento:*** il trattamento dei dati personali è legittimo solo nel caso in cui sussista almeno una delle seguenti condizioni: la persona cui appartengono ha dato il suo consenso per uno o molteplici scopi; è necessario per un contratto di cui la persona cui appartengono è o sarà parte; è necessario per compiere un dovere legale (es. pagamento di tasse per un'azienda); è necessario per fini di interesse pubblico o per conto delle autorità; è necessario per interessi legittimi (o di una terza parte), tranne nei casi in cui vengano lesi gli interessi, i diritti fondamentali e le libertà della persona cui appartengono.
- ***Trasferimenti internazionali:*** il GDPR mantiene il divieto generale di inviare dati personali al di fuori dello Spazio economico europeo in Paesi che non forniscono adeguata protezione. Al momento della scrittura di questo documento, quella di seguito è la lista dei Paesi che la Commissione europea ritiene forniscano un'«adeguata» protezione: aziende statunitensi autocertificate in base all'accordo UE-USA detto«scudo per la privacy» (si noti che ciò non fa degli Stati Uniti un Paese che fornisce protezione adeguata), Andorra, Argentina, Canada (limitatamente alla legge PIPEDA), Isole Faroe, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera e Uruguay. Nei casi in cui non è stata emessa nessuna decisione circa l'adeguatezza della protezione offerta, è possibile trasferire i dati solo in circostanze limitate, sulla base del consenso, dell'uso di clausole contrattuali standard pubblicate dalla Commissione europea o, in caso di trasferimento tra aziende, facendo ricorso a Binding Corporate Rules.

Cosa potete fare subito

- Per saperne di più visitate l'area dedicata alla riforma sulla protezione dei dati del sito web dell'ICO dove sono disponibili varie guide e informazioni generali. In particolare, consigliamo di consultare la pubblicazione ICO intitolata «Preparing for the General Data Protection Regulation—12 steps to take now».
- Rivedete i vostri sistemi di raccolta e trattamento dei dati personali per accertarvi che siano in linea con il GDPR. Potete anche valutare la possibilità di effettuare, tra gli altri, dei controlli sul piano legale e tecnologico relativamente al GDPR.
- Accertatevi che i vostri dipendenti e partner siano a conoscenza del GDPR e predisponete una formazione adeguata per prepararli. Ricordate che, in base al GDPR, sarete responsabili anche per le terze parti addette per vostro conto al trattamento dei dati.
- Avvaletevi di una consulenza legale per capire meglio le ripercussioni del GDPR sulla vostra azienda.

Per maggiori informazioni, visitate il sito: sage.com/RGPD

Dichiarazione di non responsabilità di Sage

Le informazioni contenute in questa guida sono da intendersi per fini puramente indicativi e non devono, in alcun modo, essere intese come sostitutive di un'appropriata assistenza legale. Sage tiene a ribadire ai suoi clienti che, in caso di incertezza riguardo alle potenziali ripercussioni del GDPR sulla propria azienda, è opportuno effettuare ricerche personali e approfondite sull'argomento o richiedere una consulenza legale.

Nonostante gli sforzi per garantire la correttezza e l'attualità delle informazioni contenute in questo sito web, Sage non può garantirne la completezza o l'accuratezza, fornendole perciò senza alcun tipo di garanzia, espressa o implicita. Sage non accetta nessuna responsabilità per errori o omissioni e non potrà essere ritenuta responsabile per eventuali danni (compresi, a titolo esemplificativo e non esaustivo, danni per perdita di profitti o lavoro) derivanti da contratto, torto o altro utilizzo di queste informazioni o da qualsiasi azione o decisione presa come risultato dell'uso di queste informazioni.

© 2017 The Sage Group plc o sue licenziatarie. Sage, i loghi Sage nonché i nomi di prodotti e servizi Sage menzionati in questo documento sono marchi registrati di proprietà del gruppo The Sage Group plc o di sue licenziatarie. Tutti gli altri marchi sono proprietà dei rispettivi proprietari.