PASSI CONCRETI VERSO il GDPR

con Fellowes Brands™

Che cosa comporta per te e la tua azienda la nuova regolamentazione europea per la protezione dei dati?

NASCONDI

I DATI SULLO SCHERMO
DA OCCHI CURIOSI

CONSERVA

I DATI IN MODO SICURO

DISTRUGGI

I DATI COMPLETAMENTE
ED EFFICACEMENTE

Cordery®
Legal.Compliance

Che cos'è e cosa cambierà

L'Unione Europea (UE) ha modificato le norme sulla protezione dei dati. Le modifiche sono ora legge ed entreranno in vigore in tutta l'UE il 25 maggio 2018. Le nuove norme sono denominate Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) e si applicano a tutti, dalle autorità pubbliche alle piccole e medie imprese. Tali modifiche influenzeranno il modo in cui operiamo nel nostro business.

Con la presente informativa intendiamo offrire una presentazione generale del GDPR e spiegare, in particolare, in che modo influenzerà il nostro lavoro.

Cos'è la protezione dei dati dell'UE?

Nell'UE sono in vigore norme giuridiche per la raccolta e il trattamento dei dati personali. Chiunque raccolga o tratti dati personali deve proteggerli da qualsivoglia uso improprio e rispettare una serie di disposizioni legislative. Il GDPR aggiorna le norme oggi in vigore.

Queste nuove norme si applicano ai dati detenuti in forma elettronica e cartacea?

Sì. Il GDPR si applicherà ai dati detenuti in forma sia elettronica (come e-mail e database) che cartacea (con poche eccezioni). Ciò significa che siamo responsabili anche degli archivi cartacei: dobbiamo conservarli in modo sicuro e distruggerli in sicurezza (ad esempio utilizzando un distruggidocumenti sicuro) quando non sono più necessari.

Multe fino a
€20 milioni
di euro oppure il 4% del volume d'affari globale annuo di un'azienda

In quali tipi di sanzioni può incorrere un'azienda in caso di violazione delle norme?

In base alle nuove norme in materia di protezione dei dati, le autorità competenti possono imporre sanzioni elevate in caso di violazioni. La sanzione può raggiungere i 20 milioni di euro oppure il 4% del volume d'affari globale annuo di un'azienda, a seconda di quale importo è maggiore. Anche se non tutte le violazioni porteranno alla sanzione più elevata, vedersi comminare una sanzione, sia pure minima, non è un'opzione ammissibile: il rispetto delle norme da parte di tutti è fondamentale.

Le aziende dovranno fare di più?

Sì. In base alle nuove norme, ogni azienda avrà maggiori responsabilità e obblighi. In particolare, alle aziende viene richiesto di adottare misure tecniche e organizzative a garanzia del trattamento corretto dei dati. Per valutare il corretto livello di sicurezza è necessario considerare i rischi connessi al trattamento dei dati, in special modo quelli legati a una distruzione accidentale o illegale. Occorre anche essere in grado di dimostrare quali misure sono state intraprese in caso di controlli da parte delle autorità competenti. Una parte significativa, sotto questo aspetto, consiste nel controllare a chi

Vi sono esempi di casi in cui sono stati commessi degli errori?

- **La mancata conformità può avere conseguenze particolarmente dolorose**. Recentemente l'autorità di controllo in materia di protezione dei dati del Regno Unito, l'Information Commissioner's Office (ICO), ha inflitto a un ente locale una sanzione di 100.000 sterline per non aver messo in atto misure appropriate per difendersi dalla perdita o dalla distruzione accidentale dei dati. Dei documenti contenenti dati personali di circa 100 persone (inclusi adulti e bambini in situazioni vulnerabili) erano infatti stati trovati dall'acquirente di un edificio abbandonato precedentemente utilizzato dall'ente locale. In pratica, quando l'ente locale aveva trasferito gli uffici, aveva abbandonato alcuni dei documenti nell'edificio occupato in precedenza.

- In Olanda alcuni operatori del trasporto pubblico sono stati sanzionati dall'autorità competente in materia di protezione dei dati perché avevano conservato più a lungo del necessario i dati relativi ad alcune transazioni. Agli operatori era stato inizialmente richiesto di provvedere a distruggere o rendere anonimi tali dati e in effetti gli operatori avevano optato per renderli anonimi. Tuttavia, le tecniche di anonimizzazione sono risultate insufficienti in almeno un caso e, di conseguenza, un operatore ha dovuto pagare una multa pari a 125.000 euro.

- In Spagna vi sono stati alcuni casi di applicazione di sanzioni da parte dell'autorità competente in materia di protezione dei dati quando documentazione contenente dati personali è stata gettata nei cestini dei rifiuti o per strada. In almeno un caso, la documentazione era stata distrutta solo parzialmente, mentre in altri casi lo smaltimento nella spazzatura era dovuto alla mancata distruzione o alla distruzione non corretta di tali documenti.

vengono inviati i dati personali: ad esempio sarà necessario verificare anche le procedure adottate dalle aziende con cui si collabora,

Dovremo mettere la protezione dei dati al centro di ciò che facciamo?

Sì. Il rispetto della privacy dovrà essere integrato in tutti i processi aziendali. Le aziende dovranno mettere in atto misure idonee per essere sicure di elaborare solo i dati personali strettamente necessari. Ogni addetto dovrà chiedersi:

- Questi dati personali mi servono veramente?
- È necessario elaborarli per questo scopo?
- Tutti quelli che hanno accesso ai dati hanno realmente necessità di accedervi (ad esempio, se solo gli addetti alle risorse umane dovrebbero visionare certi documenti, questi dovrebbero essere chiusi in un casellario di cui solo il reparto Risorse Umane ha le chiavi)?

I dati non più necessari dovrebbero essere **distrutti in modo sicuro**

Sarà necessario il consenso per il trattamento dei dati?

Sì. In via generale, deve esservi un motivo legittimo per poter elaborare dei dati personali. Se è necessario il consenso al trattamento dei dati, secondo le nuove norme, questo deve essere fornito liberamente, deve essere specifico, informato e inequivocabile. Il silenzio, il diritto di opt-out (ritirare il consenso) o l'inattività non possono essere invocati; deve, invece, essere messa in atto una procedura attiva come la spunta di una casella. Le aziende devono anche essere in grado di dimostrare che il consenso è stato effettivamente fornito. È quindi indispensabile assicurarsi di aver adottato procedure che rispettino tutti questi requisiti.

Sono stati introdotti nuovi diritti?

Sì. È stata introdotta una serie di nuovi diritti inclusi:

- il "diritto all'oblio", che consente alle persone di richiedere la cancellazione dei propri dati personali;
- il "diritto alla portabilità dei dati", che consente alle persone di richiedere la conservazione dei propri dati personali in un formato comunemente usato per il trasferimento; e
- il "diritto di opposizione", che include la possibilità per gli interessati di opporsi alla creazione di profili dai dati personali. È inoltre possibile opporsi al trattamento dei dati personali per il marketing diretto.

L'implementazione delle nuove norme costituirà una sfida per le aziende, anche se occorre puntualizzare che tutti questi nuovi diritti sono con riserva, cioè vi sono alcune eccezioni per le quali è necessaria una consulenza legale.

Come si affronta il caso di persone che chiedono di visionare i propri dati?

Il diritto degli interessati a visionare i propri dati, tecnicamente chiamato "richiesta di accesso da parte dell'interessato" (SAR, Subject Access Request), è previsto anche dalle nuove norme. Consente a chiunque di esercitare il diritto a ottenere l'accesso ai dati sulla propria persona detenuti da un'azienda o ente pubblico. Secondo le nuove norme, il titolare del trattamento deve rispondere alle richieste di accesso ai dati entro un mese dalla ricezione delle stesse (sebbene sia possibile, in alcune circostanze, un'estensione per un massimo di due ulteriori mesi), mentre la possibilità da parte del titolare del trattamento di chiedere un contributo è stata abolita. Negli ultimi anni vi è stata una crescita significativa nel numero di richieste di accessi ai dati presentate; nel momento in cui diventeranno gratuite, c'è da aspettarsi una crescita ancora maggiore. E con l'aumento delle applicazioni di posta elettronica e cloud, le richieste di accesso ai dati personali sono adesso ancora più costose e complesse.

Una parte fondamentale della futura strategia di protezione dei dati di qualsiasi azienda sarà pertanto quella di mettere in atto procedure adeguate per affrontare le richieste di accesso ai dati personali.

Dovrò nominare un responsabile della protezione dei dati?

Può darsi. Secondo il GDPR gli enti pubblici sono obbligati a nominare un Responsabile della protezione dei dati e, in alcune circostanze, anche le aziende che hanno a che fare con la compliance in materia di protezione dei dati dovranno fare altrettanto. Anche in questo caso, è consigliabile richiedere una consulenza legale specifica che tenga conto delle attività che si svolgono e del luogo in cui sono svolte. Data l'importanza oggi assunta dal rispetto della

privacy, anche se tecnicamente parlando un responsabile della protezione dei dati potrebbe non essere necessario, un'azienda di medie dimensioni che tratta regolarmente dati personali dovrebbe tuttavia prendere in considerazione di nominarne uno.

Dovrò segnalare eventuali violazioni dei dati?

Sì. La garanzia della sicurezza dei dati è una delle colonne portanti delle nuove norme e include le problematiche relative alla segnalazione delle violazioni dei dati.

> Ciò che costituisce una violazione dei dati comprende varie situazioni, che includono distruzione, perdita, alterazione, divulgazione non autorizzata dei o accesso ai dati personali.

Le violazioni (insieme alle azioni intraprese per ridurne le conseguenze) dovranno essere segnalate all'autorità competente per la protezione dei dati senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne è venuti a conoscenza. Anche l'interessato deve essere informato della violazione dei dati personali senza ingiustificato ritardo (ma non è stato stabilito un tempo limite ufficiale) qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica. Sono previste alcune limitate eccezioni alla segnalazione e all'informazione degli interessati per le quali è necessario richiedere un'adeguata consulenza legale.

La segnalazione della violazione dei dati personali è resa ancora più complicata da alcuni fattori:

- in alcuni Paesi (inclusi Austria, Germania e Paesi Bassi) sono già in vigore obblighi relativi alla segnalazione delle violazioni dei dati;
- la segnalazione delle violazioni dei dati può essere obbligatoria ai sensi di altre regolamentazioni e normative, in particolare nei settori finanziario e sanitario; e
- una legislazione aggiuntiva separata dovrà essere implementata all'interno della UE in linea con la Direttiva UE sulla Cyber Security.

Le aziende devono perciò mettere in atto un piano di azione ben definito e una politica chiara sulla violazione dei dati come priorità assoluta e formare il personale.

Quali sono le novità per quanto riguarda responsabilità e risarcimento?

Come principio generale, chi ha subito un danno a causa di una violazione delle nuove norme ha diritto, con alcune eccezioni, a richiedere il risarcimento al titolare del trattamento e al responsabile del trattamento dei dati personali in questione. A causa del rischio supplementare che un'infrazione delle nuove norme può adesso comportare, in special modo in caso di violazione dei dati personali, le aziende dovranno fare il massimo per contenere il rischio potenziale di richieste di risarcimento.

Sarà necessario effettuare delle valutazioni dell'impatto sulla privacy?

Sì. Secondo le nuove norme, tali valutazioni sono denominate "Valutazioni d'impatto sulla protezione dei dati" (DPIA, Data Protection Impact Assessment). Dovrà essere eseguita una valutazione dell'impatto delle operazioni di trattamento proposte sulla protezione dei dati personali laddove le operazioni di trattamento dei dati (in particolare quelle che impiegano nuove tecnologie) siano suscettibili di comportare un elevato rischio per i diritti e le libertà delle persone fisiche. Tale valutazione deve essere effettuata prima del trattamento. Deve poi essere consultata un'autorità competente per la protezione dei dati (sempre prima del trattamento) laddove una valutazione indichi che il trattamento potrebbe portare a un rischio elevato in assenza di misure per contenerlo.

Queste valutazioni diverranno probabilmente comuni e dovrebbero risultare uno strumento molto utile per le aziende per affrontare i rischi per la privacy, incluse la valutazione del rischio per la sicurezza dei dati e la considerazione dei rischi connessi al trattamento dei dati personali come la distruzione accidentale o illegale

È cambiato qualcosa sotto il profilo dei trasferimenti di dati in Paesi terzi?

Non molto. Con il GDPR rimangono in vigore le norme speciali vigenti in materia di trasferimento dei dati dagli Stati membri dell'UE a Paesi terzi (USA compresi), tra cui l'obbligo che tali trasferimenti possano avvenire solo laddove i Paesi terzi in questione assicurino un adeguato livello di protezione. In base al nuovo regime, tali norme sono semplicemente più dettagliate. Si tratta di un argomento complicato, oggetto inoltre di sviluppi in base alle norme vigenti sulla protezione dei dati, di cui è opportuno discutere con il proprio team legale.

Dove posso trovare maggiori informazioni?

Cosa devo fare ora?

Per mettersi in regola con il GDPR occorre mettere a budget e pianificare risorse adeguate (comprese quelle IT). È necessario mettere bene a frutto il tempo disponibile per apportare gli adeguamenti opportuni. Di seguito sono elencate le dieci questioni principali in materia di conformità di cui iniziare a occuparsi.

1. Mettere in atto un processo di valutazione dell'impatto sulla privacy: mappare i propri dati e determinare le aree di rischio.
2. Riesaminare approfonditamente i contratti con i fornitori: occorrerà la collaborazione dei fornitori, specialmente nel riferire tempestivamente i casi di violazioni della sicurezza, e pertanto è necessario assicurarsi di avere i diritti contrattuali per pretenderla.
3. Aggiornare i sistemi e i materiali e preparare registri e documentazione nuovi e dettagliati da produrre in caso di ispezione delle autorità di controllo.
4. Riesaminare gli aspetti pratici chiave, compresa la conservazione di tutti i dati utilizzati dall'azienda.
5. Assicurarsi di disporre di piani per distruggere in sicurezza i dati di cui non si ha bisogno.
6. Assicurarsi che i nuovi aspetti come il "consenso esplicito", il "diritto all'oblio", il "diritto alla portabilità dei dati" e il "diritto di opposizione" siano inclusi nelle policy e nelle procedure.
7. Istituire una procedura per la segnalazione delle violazioni dei dati, che comprenda capacità di rilevamento e reazione e testarla come avviene per le prove antincendio.
8. Valutare l'opportunità di nominare un responsabile della protezione dei dati.
9. Formazione, formazione, formazione: formare il personale su tutto quanto descritto sopra (le autorità competenti in materia di protezione dei dati prestano molta attenzione a questo aspetto).
10. Impostare e intraprendere regolari controlli sulla compliance per identificare e risolvere tempestivamente i problemi.

Esperienza

Jonathan Armstrong e **André Bywater** di **Cordery Compliance** vantano una vasta esperienza nella consulenza su questioni relative al GDPR e hanno contribuito alla stesura del presente White Paper.

www.corderycompliance.com

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street,
London, EC4A 4HH
+44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

André Bywater
Cordery
Lexis House
30 Farringdon Street
London, EC4A 4HH
+44 (0)207 075 1785
andre.bywater@corderycompliance.com

A proposito di Fellowes: a missione di Fellowes è fornire soluzioni innovative per la postazione di lavoro, in grado di aiutare a lavorare in sicurezza, comodamente e produttivamente, in particolare **macchine per ufficio, prodotti ergonomici e soluzioni per la gestione degli archivi.**

www.fellowes.com

Fellowes Ltd
Fellowes Leonardi spa
Via Direttissima del Conero 27
60021 Camerano (AN)
info@fellowesleonardi.it

Cordery® Legal.Compliance

Fellowes Brands™