MONTORO & PARTNERS

COMMERCIALISTI

Salerno 08 Maggio
Ai Signori Clienti
Loro Sedi

CIRCOLARE 03/2018

- ✓ Violazione dei dati personali (data breach): gli adempimenti previsti

Il nuovo Regolamento (Ue) 2016/679 prevede una serie di adempimenti da svolgere nel caso in cui i dati personali conservati, trasmessi o trattati da aziende e Pubbliche Amministrazioni siano soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. In determinati settori vi è, infatti, l'obbligo di comunicare eventuali violazioni di dati personali (data breach) all'Autorità stessa e, in alcuni casi (nei casi più gravi), anche ai soggetti interessati.

L'art. 33 del Regolamento Europeo introduce l'obbligo di notifica della violazione dei propri sistemi informatici, ossia un data breach, al Garante della Privacy ed estende inoltre all'interno dell'art. 34 tale notifica a tutti gli interessati in caso di "rischio elevato". La notifica va effettuata entro 72 h e comunque "senza giustificato ritardo" da quando il titolare è venuto a conoscenza della violazione.

Scadenza :

- 25.05.2018

Riferimenti Normativi

- Nuovo Regolamento Ue 679/2016

Premessa

Il nuovo Regolamento (Ue) 2016/679 negli artt. da 32 a 34 prevede una serie di adempimenti da svolgere nel caso in cui i dati personali conservati, trasmessi o trattati da aziende e Pubbliche Amministrazioni siano soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

Il titolare del trattamento, in particolare è obbligato secondo l'art. 33 del Regolamento alla notifica al Garante della violazione dei propri sistemi informatici, ossia un data breach, al Garante della Privacy ed estende inoltre all'interno dell'art. 34 tale notifica a tutti gli interessati. Entro 72 h e comunque "senza giustificato ritardo" da quando il titolare è venuto a conoscenza della violazione.
Oltre le 72 h, tale comunicazione dovrà essere accompagnata dalle ragioni del ritardo nell'agire.

OBBLIGO NOTIFICA - Art.33

- Al Garante della Privacy entro 72 h e comunque "senza giustificato ritardo" da quando si è venuti a conoscenza della violazione ai propri sistemi informatici.

OBBLIGO NOTIFICA – Art.34

- A tutti gli interessati in determinati casi se il titolare ritiene che il rischio per i diritti e le libertà degli interessati sia elevato.

Quando va effettuata la notifica al Garante

Può, infatti, accadere che in qualsiasi azienda ci sia un incidente di sicurezza in cui i dati sensibili, protetti o riservati vengano consultati, copiati, trasmessi, rubati o utilizzati da un soggetto autorizzato o addirittura di essere protagonisti di attacchi informatici compromettendo la sicurezza dei propri sistemi. Un data breach può essere anche la perdita di una chiavetta USB o la sottrazione di documenti con dati personali.

DATI VIOLATI POTREBBERO AD ESEMPIO RIGUARDARE:

↘**l'ambito finanziario**, ad esempio dati di carte di credito e di conti correnti;

↘**l'ambito sanitario**, ad esempio informazioni sulla salute personale e malattie;

↘**proprietà industriale**, ad esempio segreti commerciali, brevetti, documentazione riservata, lista clienti, progetti finalizzati ad esempio a pratiche di concorrenza sleale;

↘**personali,** ad esempio dati di documenti di identità, codici personali ecc.

Soluzioni Preventive

Il titolare è obbligato a mettere in atto tutte le soluzioni, tutte le misure necessarie ab origine affinché una tale situazione non possa mai verificarsi in azienda o in qualsiasi studio professionale, secondo il principio, infatti, del privacy by design ovvero del "prevenire anziché correggere".

Obblighi Titolare

- porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato;
- la riservatezza dei dati (inteso come il dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento);
- garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente.

Secondo il principio del privacy by design ovvero del "prevenire anziché correggere".

Contenuto della notifica

Per quanto riguarda il contenuto della notifica secondo l'art. 33 del GDPR deve almeno contenere le informazioni minime sotto descritte.

- Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Descrivere le probabili conseguenze della violazione dei dati personali;
- Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il nuovo Regolamento (Ue) 2016/679 insieme ai provvedimenti adottati del Garante della privacy prevedono una serie di adempimenti da svolgere nel caso in cui i dati personali conservati, trasmessi o trattati da aziende e Pubbliche Amministrazioni siano soggetti al rischio di perdita, distruzione o diffusione indebita, come nei casi sopra descritti, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

Sintesi Adempimenti Data Breach

Adempimenti che potremmo sintetizzare in 5 punti:

- Rilevare la violazione e informare il titolare e il responsabile del trattamento;
- Gestire e valutare l'entità della violazione;
- Avviare le procedure per la notifica al Garante;
- Avviare le procedure per l'eventuale comunicazione agli interessati (solo quando i rischi sono considerati "elevati");
- Registrare e documentare la violazione avvenuta.

Obbligo di comunicazione all'interessato

Se il titolare ritiene che il rischio per i diritti e le libertà degli interessati sia elevato, allora, secondo i casi indicati dall'art. 34, dovranno essere informati anche gli interessati del data breach, descrivendo con un linguaggio chiaro e semplice la natura della violazione contenendo le informazioni dell'art. 33 sopra descritte e le misure adottate.

NON È OBBLIGATORIA INVECE LA COMUNICAZIONE ALL'INTERESSATO SE È SODDISFATTA UNA DELLE SEGUENTI CONDIZIONI:

- Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

- Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

- La comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Sanzioni

Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative, il cui importo può arrivare fino a 10 milioni di euro o, se superiore, al 2% del fatturato totale annuo dell'esercizio precedente.

In ogni caso tutte le misure adottate da parte del DPO o del titolare del trattamento dovranno essere opportunatamente documentate tramite un apposito registro delle violazioni, anche nei casi di comunicazioni non inviate al Garante. Tale documentazione dovrà essere poi disponibile in caso di accertamenti.

Possibili soluzioni preventive

Diverse le tecniche che potrebbero essere adottate all'interno di un sistema di sicurezza, dalla cifratura dei dati e degli archivi alla pseudonimizzazione (l'utilizzo e la conservazione dei dati in maniera separata) secondo il concetto di "privacy by design", ovvero "prevenire non correggere" un approccio diverso a tutto il sistema di prevenzione definito dall'art. 25 del Regolamento, un approccio cioè concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

Nel Considerando 83 viene indicata infatti la cifratura delle informazioni quale sistema di sicurezza da adottare. In termini molto semplici la cifratura non è altro che una modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale.

Mentre la pseudonomizzazione dei dati prevede che le informazioni debbano essere conservate in una forma che ne impedisca l'identificazione dell'utente. In tal modo qualora si verificasse un incidente come quelli sopra descritti chi ne venisse in possesso non potrebbe utilizzarli o comunque essere in grado di consultarli o associarli ad alcuno senza avere informazioni aggiuntive.

La prevenzione di data breach passa dunque dalla valutazione dei rischi e dalla definizione di misure di tipo tecnologico e organizzativo, attraverso, ad esempio, l'utilizzo anche di audit interni finalizzati a verificarne la validità e la conformità di tutto il processo, la definizione di policy del personale e la creazione di un incident responce per far fronte agli incidenti qualora si verificassero.

Cordiali Saluti

Montoro &Partners