ADOS SRL
CONSULENZE PER L'IMPRESA

Audit - Data protection – Outsourcing Services

Lunedì 17 giugno 2019

A tutti i clienti

SICUREZZA INFORMATIVA DEI DATI PERSONALI

In linea generale suggeriamo di effettuare le seguenti attività di verifica:

- Controllo dell'esattezza e dell'aggiornamento di tutti i dati personali trattati presenti nelle banche dati;
- Verifica di coerenza sui tempi di conservazione dei dati personali con quanto indicato nel registro dei trattamenti e nelle informative rese agli interessati;
- Previsione di idonee tecniche di reazione al *data breach,* in una logica di *business continuity*.

Con l'occasione invitiamo i Titolari a verificare l'adozione almeno dei seguenti standard di sicurezza:

- Applicare il principio del minimo privilegio;
- Crittografare i dati sensibili con tecniche di cifratura;
- Prevedere sistemi di autenticazione a due fattori;
- Effettuare adeguata formazione IT tra gli addetti al trattamento;
- Adottare tecniche di pseudonimizzazione dei dati;
- Vietare in via regolamentare l'utilizzo di e-mail ordinaria per la trasmissione dei dati particolari (ex dati sensibili);
- Utilizzare sistemi di posta crittografata;
- Evitare trasmissione di dati particolari via telefax;
- Evitare l'utilizzo di prodotti di terze parti (ad es. *we transfer*) per la trasmissione di dati particolari;
- Prevedere sistemi aziendali di *file sharing*;
- Vietare l'archiviazione di dati particolari su hard disk del pc e utilizzare per l'archiviazione soltanto il server aziendale;
- Evitare utilizzo di chiavette USB e hard disk esterni per archiviare dati particolari;
- Prevedere una *policy* severa per le credenziali di autenticazione;
- Inventariare periodicamente le risorse informatiche aziendali e i software installati;
- Prevedere nei regolamenti aziendali per l'utilizzo delle risorse informatiche adeguate sanzioni disciplinari in caso di inosservanze.

Ricordiamo che l'adozione di una adeguata *policy* a livello dei sistemi informativi è condizione indispensabile per realizzare la GDPR *compliance* ed evitare l'irrogazione di sanzioni pecuniarie.

In tale ambito suggeriamo ai Titolari del trattamento di commissionare un **audit esterno ed indipendente** sul proprio sistema informativo e sulle misure di sicurezza informatiche adottate e a far pervenire al DPO il report di audit in modo da valutare eventuali gap o non conformità.

Infine suggeriamo ai Titolari di stipulare idonee polizze di assicurazione cd. "cyber risk" che possano coprire in modo idoneo gli eventuali danni derivanti da eventi avversi.