

SCHEDA N. 23 – VIOLAZIONE DEI DATI – DATA BREACH

VIOLAZIONE DEI DATI – DATA BREACH

→ **Regolamento (Ue) 2016/679 – Artt. da 32 a 34**

→ 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, 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, anche ai soggetti interessati

I 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.

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

CONTENUTO NOTIFICA

- 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.

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 di cui al paragrafo 1;
- 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.