MODULO DI RISK ASSESSMENT - VIOLAZIONE DATI PERSONALI

Risk Assessment	Descrizioni e Note
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei i settori aziendali (indicare quali):	
I dati particolari coinvolti (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: a) origine razziale o etnica; b) opinioni politiche, convinzioni religiose o filosofiche; c) appartenenza sindacale; d) dati genetici; e) dati biometrici; f) dati giudiziari; g) relative alla salute o all'orientamento sessuale di una persona.	

Risk Assessment	**Descrizioni e Note**
Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito)	
Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori)	
Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	
Notificazione del Data Breach all'Autorità Garante	
Comunicazione del Data Breach agli interessati	
Comunicazione del Data Breach ad altri soggetti	