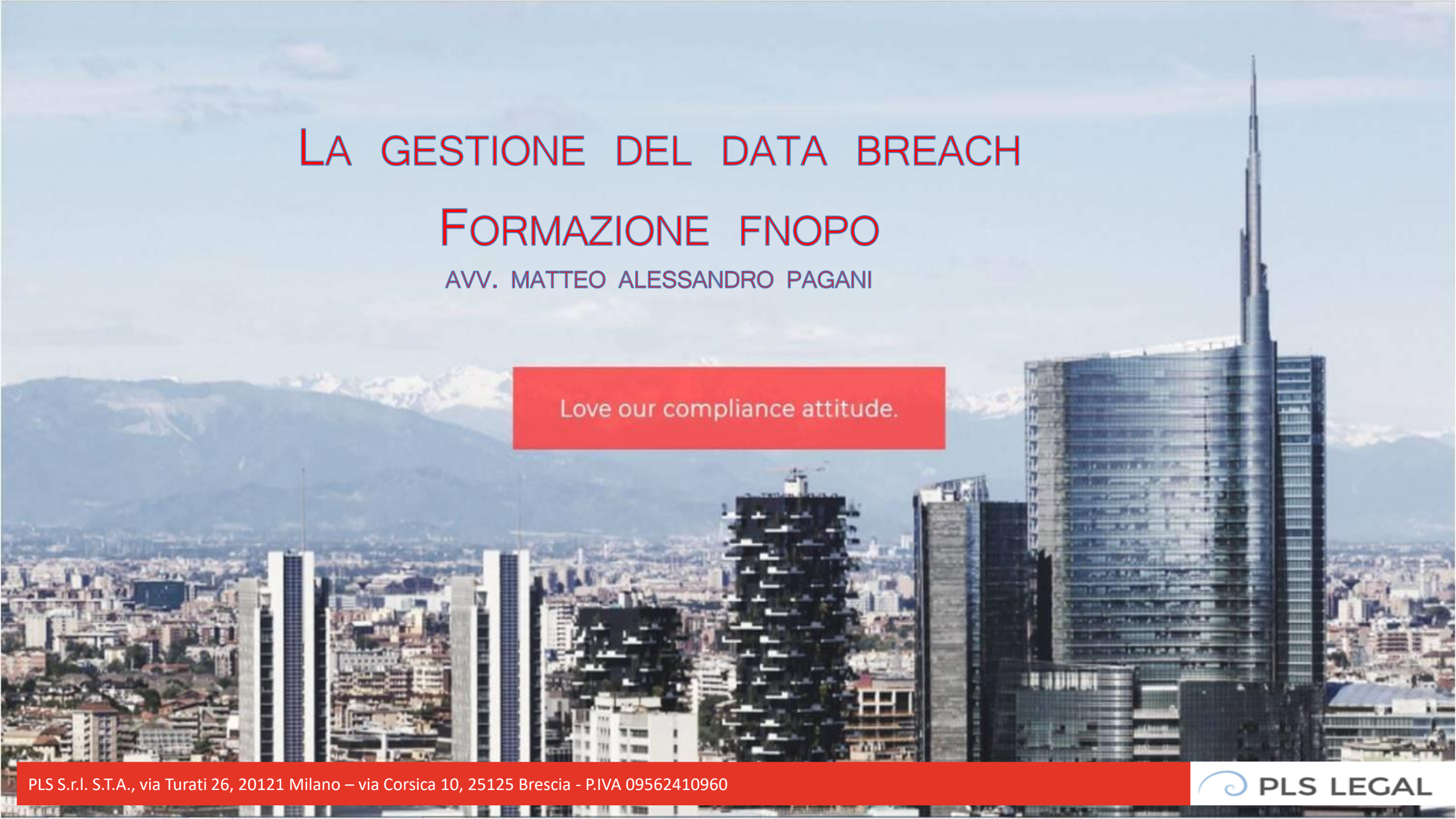


LA GESTIONE DEL DATA BREACH

FORMAZIONE FNOPO

AVV. MATTEO ALESSANDRO PAGANI

Love our compliance attitude.

Prima di iniziare ricordiamo alcune definizioni

- **Dato personale:** ex art. 4, (1) GDPR, qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online ovvero uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- **Trattamento:** ex art. 4, (2) GDPR, qualsiasi operazione ovvero insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicata a Dati personali o insieme di Dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- **Titolare del trattamento:** ex art. 4, (7) GDPR la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di Dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Prima di iniziare ricordiamo alcune definizioni

- **Consenso dell'interessato**: ex artt. 4, (11) e 7 GDPR qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati personali che lo riguardano siano oggetto di trattamento;

- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio ovvero altro organismo che tratta Dati personali per conto del Titolare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, previo accordo giuridico o altro atto equivalente;

- **Violazione dei dati personali:** ex art. 4, (12) GDPR, la violazione di sicurezza che comporta accidentalmente ovvero in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati;

- **Data Protection Officer ("DPO"):** soggetto qualificato e previsto dall'art. 37 GDPR, nonché designato dal Titolare o dal Responsabile del Trattamento per assolvere le funzioni di consulenza, supporto e controllo previste dall'art. 39 GDPR;

- **Limitazione di trattamento:** ex art. 4, (3) GDPR, il contrassegno dei Dati personali conservati con l'obiettivo di limitarne il trattamento futuro;

- **Autorità di controllo**: ex artt. 4, (21) e 51 GDPR, l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR; L. 119/34 IT Gazzetta ufficiale dell'Unione Europea 4.5.2016 (nel caso dell'Italia si parla di «**Garante per la Protezione dei Dati Personali**»)

Sicurezza dei dati e valutazione dei rischi

Il **Titolare** del trattamento ovvero il **Responsabile** del trattamento devono **mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.**

Le misure da adottare **devono essere comunque proporzionali alla quantità ed alla qualità dei dati trattati**.

ESEMPI DI MISURE DI SICUREZZA ADEGUATE

- la pseudonimizzazione e la cifratura dei dati personali
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Sicurezza dei dati e valutazione dei rischi

Sicurezza dei dati e valutazione dei rischi

Rischi da tenere in considerazione nel valutare l'**adeguato livello di sicurezza** sono:

- derivanti dalla distruzione, dalla perdita, dalla modifica dei dati personali
- derivanti dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali

Data breach

Violazione di Dati personali o «Data Breach»: ex art. 4, (12) GDPR, la violazione di sicurezza che comporta accidentalmente ovvero in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali trasmessi, conservati o comunque trattati.

Quando si parla di «**Violazione dei Dati personali**» (art. 4, par. 12 GDPR) occorre considerare:

- **natura della violazione**:
  - accidentale o volontario;
  - illecita;
- **conseguenza sui dati:**
  - distruzione;
  - perdita;
  - modifica;
  - divulgazione non autorizzata;
  - accesso ai dati da parte di soggetti non autorizzati;
- **conseguenze sugli interessati**:
  - danni morali o immateriali;
  - perdita del controllo dei dati e conseguenti perdite economiche;
  - discriminazioni;
  - furto d'identità e frode;
  - danno reputazionale;
  - ulteriori conseguenze negative.

Data breach

ALCUNI ESEMPI DI VIOLAZIONI DI DATI PERSONALI*

*Per ulteriori esempi si veda l'Estratto (All. B) dalle Linee Guida del WP29

- computer, smartphone, memorie e dischi USB rubati persi o lasciati temporaneamente incustoditi, oppure smaltiti in modo inadeguato;
- allagamento o incendi degli archivi cartacei;
- furto smarrimento o condivisione della password o di altre informazioni di autenticazione;
- negligenza dei soggetti che trattano i Dati personali dell'ordine nell'utilizzare password semplici e facilmente identificabili;
- negligenza nel divulgare a soggetti non autorizzati informazioni protette e riservate o superficialità nel trattare e trasmettere Dati personali;
- abuso di privilegi in ambiente di rete che possono determinare modifiche ai Dati personali o installazione di software non autorizzato;
- furto di documenti cartacei contenenti informazioni personali o riservate lasciati incustoditi sulla scrivania o alla fotocopiatrice oppure smaltiti in modo inadeguato;
- inadeguate misure di sicurezza e di protezione che lasciano i sistemi vulnerabili e consentono attacchi di hacker o di organizzazioni esterne attuati mediante software che bypassano i sistemi di sicurezza, es. firewall, per accedere ai data base aziendali.

Data breach

Le **violazioni dei Dati personali** possono essere **classificate** in base alle **3 dimensioni** di RISERVATEZZA, INTEGRITÀ E DISPONIBILITÀ:

- "**VIOLAZIONE DELLA RISERVATEZZA**" si ha in caso di divulgazione o accesso non autorizzato o accidentale ai Dati personali;
- "**VIOLAZIONE DELLA DISPONIBILITÀ**" si ha in caso di perdita accidentale o non autorizzata di accesso o distruzione di Dati personali;
- "**VIOLAZIONE DELL'INTEGRITÀ**" si ha in caso di alterazione non autorizzata o accidentale dei Dati personali.

Quindi

A seconda delle circostanze, un **Data Breach** può riguardare la **riservatezza**, la **disponibilità** e **l'integrità** dei Dati personali allo stesso tempo, nonché qualsiasi combinazione di queste dimensioni.

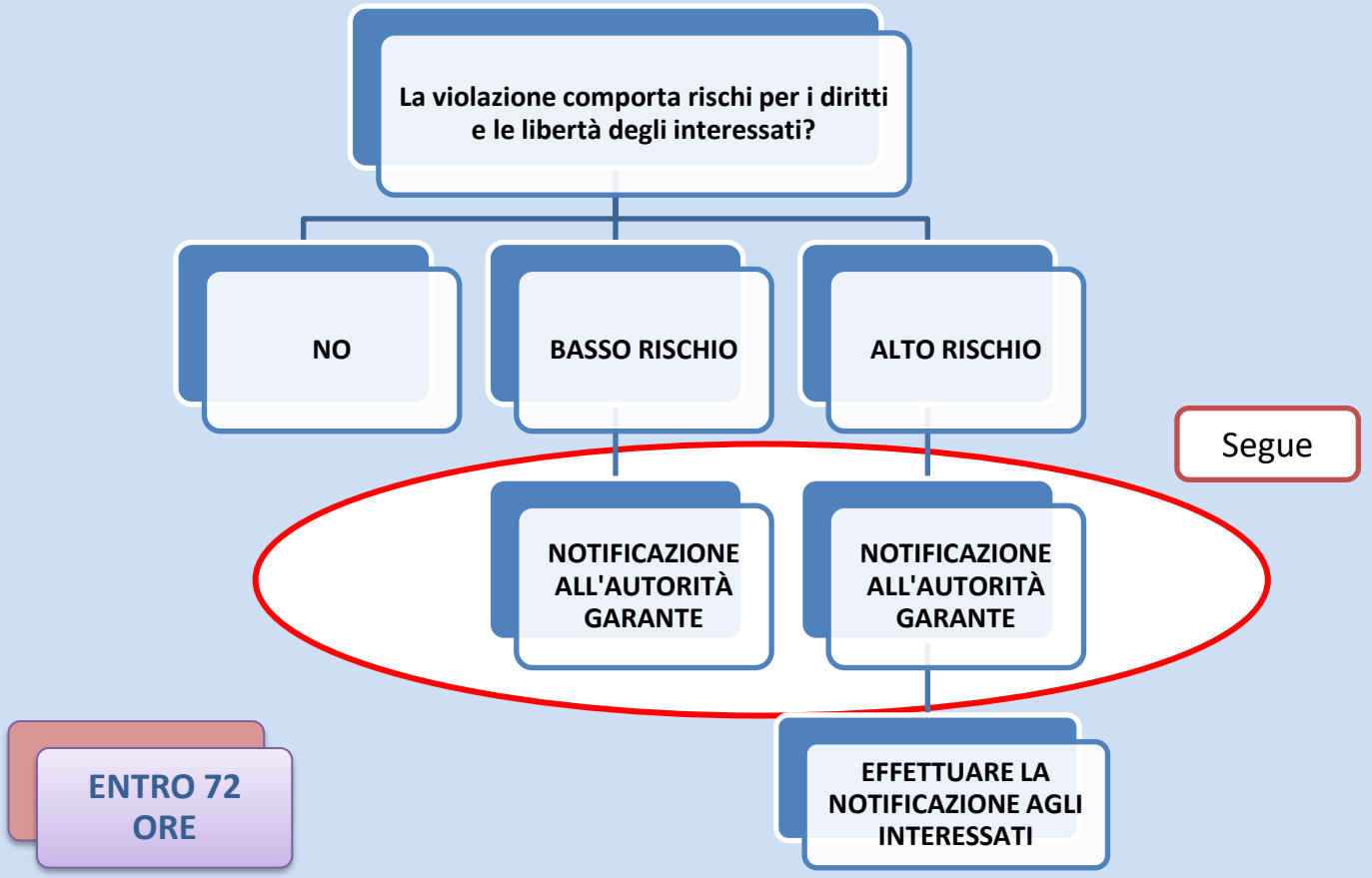
Data breach

In caso di Data Breach il Titolare dovrà valutare

- la **natura** e **l'entità** della potenziale violazione/ violazione dei Dati personali;
- **l'impatto** della violazione dati dei Dati personali;
- le **misure da adottare** per **arginare** gli effetti dannosi della violazione medesima;
- la **necessità di notifica al Garante**;
- la **necessità della notifica agli interessati**.

Data breach

Procedura che il Titolare dovrà seguire in caso di Data Breach



Data breach

NOTA BENE:
Non è richiesta notifica se la viola**zione non costituisce un probabile rischio per l'individuo**.

Il **Titolare** notifica la **violazione all'Autorità Garante** senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'Autorità Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

L'eventuale Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione

Segue

Data breach

Segue

Nel caso di violazioni di Dati personali che **presentano rischi per i diritti e le libertà degli interessati coinvolti**, il Titolare deve effettuare la **notificazione all'Autorità Garante**, riportando tutte le informazioni richieste dal suddetto art. 33 comma 3, attraverso l'apposita procedura telematica resa disponibile nel portale dei servizi online dell'Autorità Garante per la protezione dei Dati personali*.

CONTENUTO DELLA NOTIFICA ALL'AUTORITÀ GARANTE

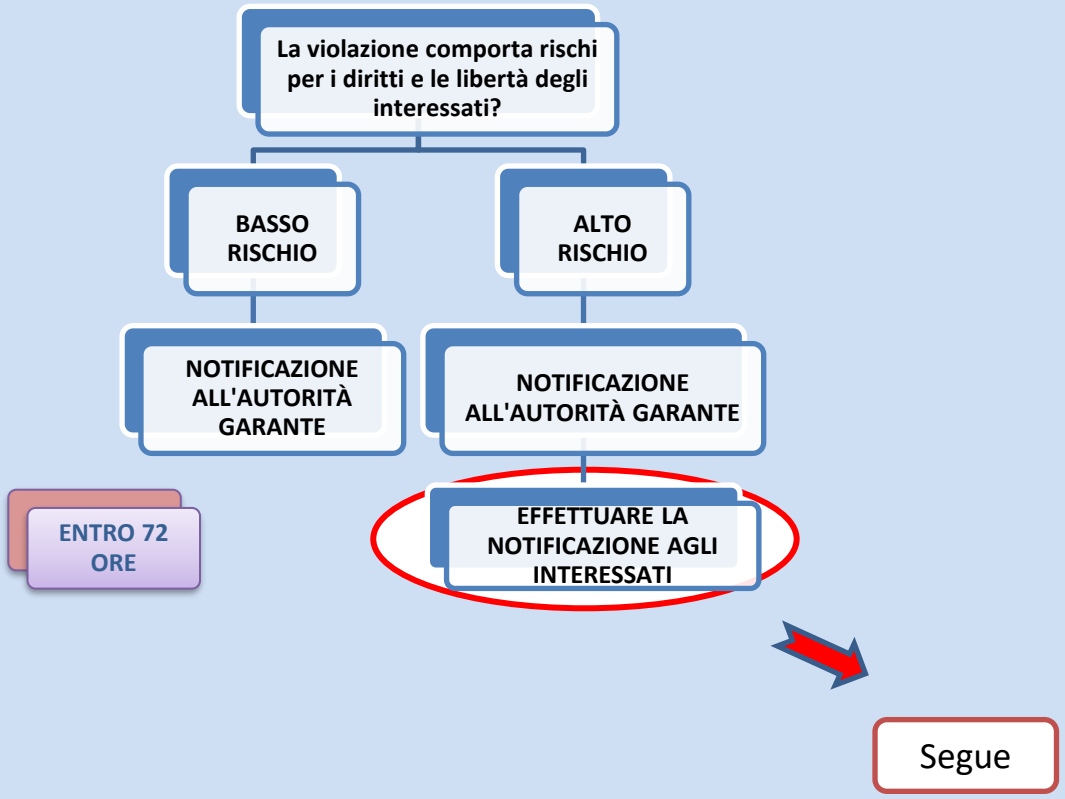
- **descrizione della natura violazione occorsa e categorie e numero interessati coinvolti**
- **dati di contatto del DPO, se nominato, o di un altro punto di contatto cui rivolgersi per avere più informazioni**
- **descrizione possibili conseguenze**
- **descrizione delle contromisure adottate/che si intende adottare**

Il Titolare del trattamento deve tenere un **registro delle violazioni** occorse e non oggetto di notifica in cui siano documentate le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

*La suddetta procedura (operante a partire dal 01/07/2021) è raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

Data breach

Nel caso di **Data Breach** che presentino **rischi elevati per i diritti e le libertà delle persone fisiche**, il Titolare del trattamento **comunica la violazione all'interessato** senza ingiustificato ritardo indicando con un linguaggio semplice e chiaro la natura della violazione dei dati personali.



Data breach

CONTENUTO MINIMO DELLA COMUNICAZIONE AGLI INTERESSATI

- **dati di contatto cui rivolgersi per avere più informazioni**
- **descrizione possibili conseguenze**
- **descrizione delle contromisure adottate/che si intende adottare**

Non è richiesta la comunicazione all'interessato in presenza di 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;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

GRAZIE PER L'ATTENZIONE