I rischi derivanti dalle nuove opPORTunità digitali nei sistemi portuali: **attacchi *cyber*** e cosa fare ai sensi del GDPR

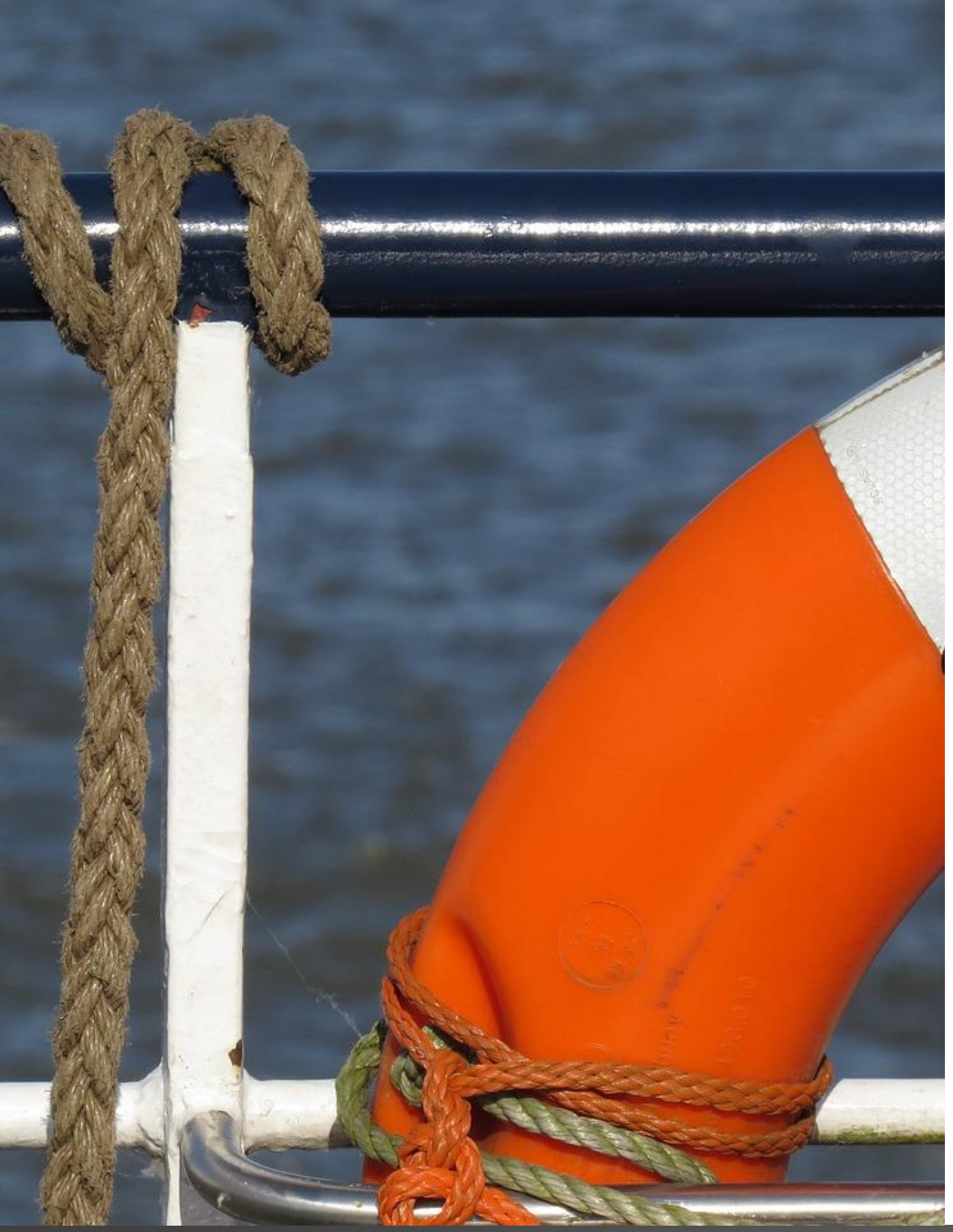
Futuro e portualità: be smart, go digital
Webinar, 27 ottobre 2020

avv. Gianluca De Cristofaro
Partner, LCA Studio Legale

Oltre al danno, la beffa…

Futuro e portualità: be smart, go digital
Webinar, 27 ottobre 2020

avv. Gianluca De Cristofaro
Partner, LCA Studio Legale



Cybersecurity portuale: flussi di dati

È un ecosistema complesso che coinvolge molteplici *stakeholders*, sistemi IT, sistemi di telecomunicazione, di controllo industriale ICS, di videosorveglianza, sensoristica, controllo accessi, illuminazione, etc., tutti tra loro interconnessi.

Possibili dati trattati nel contesto portuale:

- ✓ dichiarazioni obbligatorie alle autorità;
- ✓ dati relativi a controlli e autorizzazioni;
- ✓ dati operativi relativi a merci, servizi e operazioni portuali;
- ✓ dati finanziari (fatturazione e pagamento);
- ✓ dati di navigazione (posizione GPS e dati AIS).

Fonte – Report Enisa "Port Cybersecurity" 26 novembre 2019

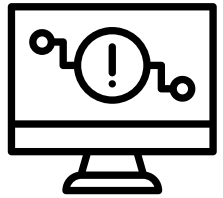
Cybersecurity portuale: tipologie di pericoli *cyber*

INTERCETTAZIONI

- Hijacking
- Intercettazioni di informazioni sensibili
- Spionaggio

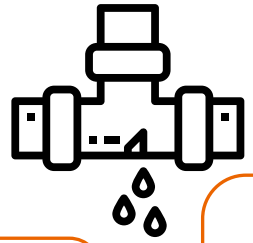
VIRUS e MALWARE

- GPS spoofing
- Denial of Service (DoS)
- Phising / social engineering
- Sottrazione e manipolazione di dati



ERRORI IT e MALFUNZIONAMENTI

- Errori ai sistemi o ai device aziendali
- Errori di terze parti (fornitori di servizi, ISP)



DANNI ACCIDENTALI

- Utilizzo di fonti e reti inaffidabili
- Cattiva amministrazione dei sistemi IT/OT
- Cancellazione fortuita di dati

ATTACCHI CYBER ALLE STRUTTURE FISICHE

- Accessi non autorizzati
- Pirateria
- Hacking e vandalismo
- Furti e frodi

Fonte – Report Enisa "Port Cybersecurity" 26 novembre 2019

Cybersecurity portuale: casi pratici

Attacchi generici ai sistemi IT o OT

- **Porto di Anversa - 2011**: violazione dei sistemi informatici del porto per acquisire informazioni su spostamento dei container;
- **Saudi Aramco - 2012**: compromissione di 35.000 computer a causa di malware contenuto in una e-mail di phishing;
- **CMA CGM - 2020**: sospetto attacco informatico ai server con possibile conseguente *data breach*.

Attacchi specifici ai sistemi portuali

- **Golfo del Messico - 2013**: compromissione dei sistemi di posizionamento e controllo della piattaforma petrolifera;
- **Maersk Attack - 2017**: attacco ramsonware all'infrastruttura IT della compagnia con blocco totale del terminal APM del porto di Rotterdam;
- **PCS Porto di Barcellona - 2018**: compromissione di alcuni server del sistema logistico portuali con conseguenti ritardi nella ricezione e consegna delle merci

La definizione “giuridica” di attacco *cyber*

Un attacco informatico (o *cyber attack*) è una qualunque **manovra**, impiegata da individui od organizzazioni anche statali, che **colpisce sistemi informativi**, **dispositivi elettronici** personali tramite atti malevoli, finalizzati al **furto**, **alterazione** o **distruzione** di dati.

Dal punto di vista della normativa in materia di protezione dati personali, un attacco *cyber* potrebbe comportare anche una **violazione di dati personali** (c.d. *data breach*).

Data breach

È un particolare tipo di incidente di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

(art. 4, par. 1, n. 12 GDPR)

Tipologie di *data breach*

Divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali

Perdita, **accesso** o **distruzione** accidentali o non autorizzati di dati personali

Modifica non autorizzata o accidentale dei dati personali

Come prevenire un *data breach* e i relativi effetti negativi?

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente ai principi e alle disposizioni in materia di protezione dei dati personali.

Come prevenire un *data breach* e i relativi effetti negativi?

Alcuni esempi di misure «adeguate» volte a evitare violazione di dati personali

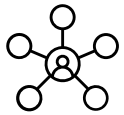
TECNICHE

Mappatura dei **dati** e delle attività di trattamento, svolgimento di ***vulnerability assessment*** sui sistemi informatici, ***penetration test*** (simulazioni di attacco contro obiettivi potenzialmente vulnerabili) e ***risk assessment*** sulle attività di trattamento svolte

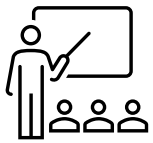
Adozione di sistemi di **crittografia** e **cifratura** dei dati, **pseudonomizzazione**, attivazione di **procedure di accesso privilegiato** alle cartelle presenti sui server aziendali o **registrazione dei *log*** ad ogni accesso da parte degli utenti, ed esecuzione regolare di backup dei dati contenuti sui server aziendali

ORGANIZZATIVE

Valutazione preventiva della ***compliance*** alla normativa sulla *data protection* dei **fornitori** (responsabili esterni del trattamento), scelta di fornitori affidabili e svolgimento di *audit* periodici sulle attività di trattamento da loro svolte



Implementazione di **policy di *data breach management*** da verificare regolarmente attraverso simulazioni di *data breach* e identificazione dei soggetti incaricati della gestione dei *data breach*

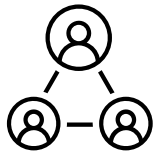


Svolgimento di attività di ***training*** del personale che svolge attività di trattamento dei dati personali e fornitura di **istruzioni operative** concernenti le modalità di trattamento dei dati personali

LCA

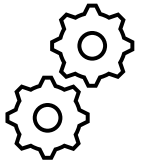

Password:
123456

Policy di *data breach management*



Individuazione dei **soggetti chiave**

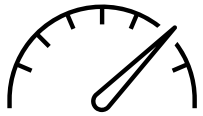
- Titolare del trattamento
- DPO (se presente)
- Responsabile IT
- Amministratori di sistema
- Referente privacy
- Designati (se individuati)



Monitoraggio delle **misure** di sicurezza implementate

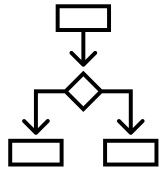
- attribuzione di nome utente e password dedicate
- software di registrazione dei *log*
- *firewall* e antivirus
- filtri web
- trasmissione dei dati su VPN crittografate

….e altre misure adeguate

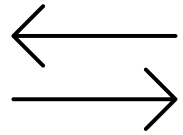


Risk assessment

- *Data protection impact assessment*



Implementazione di un **sistema** di ***assessment*** della complessità / gravità della **violazione** strutturato per fasi



Implementazione di un **sistema** di **condivisione** delle **informazioni** tra i vari soggetti coinvolti

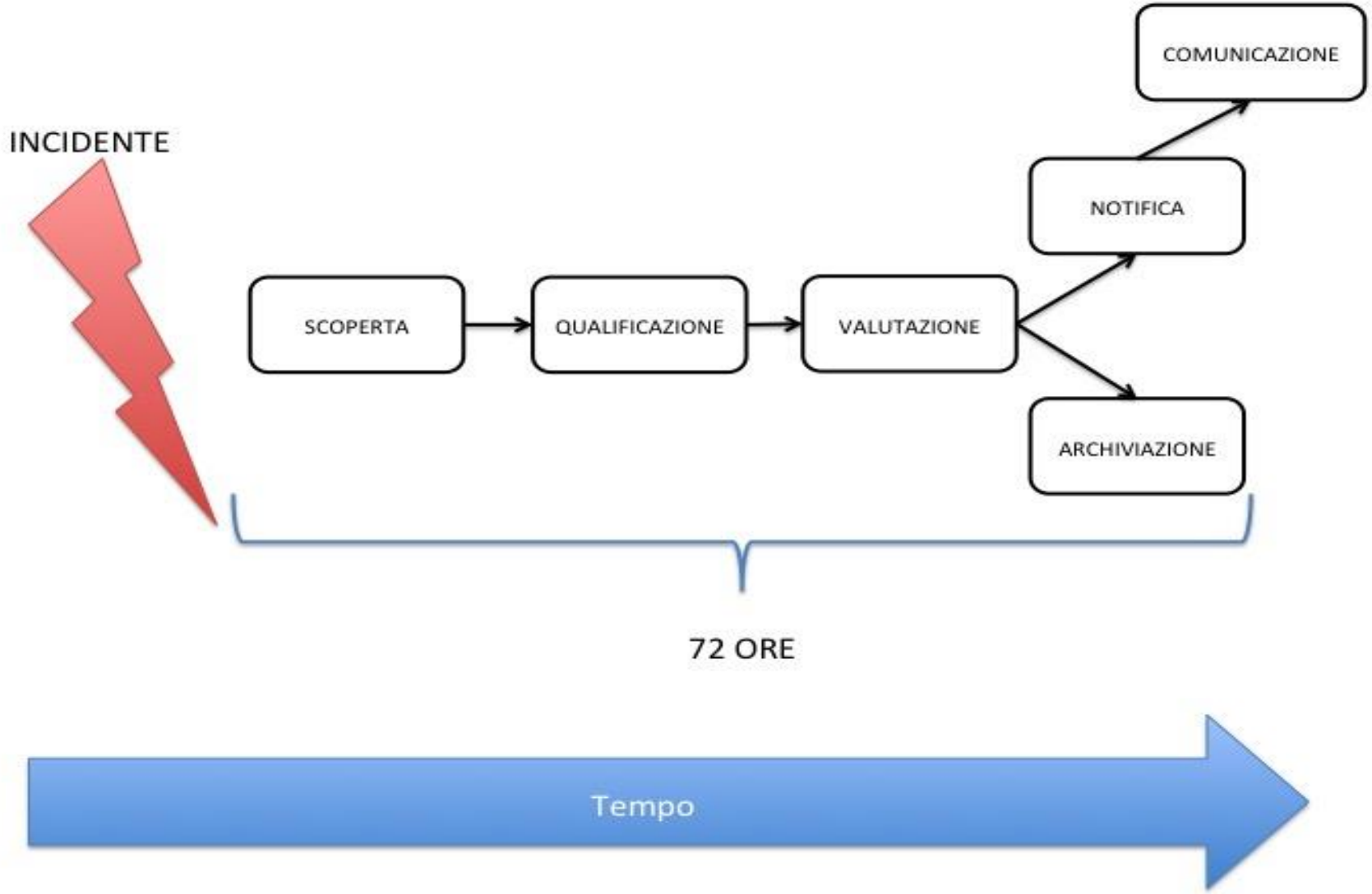
Compilazione di un **registro** dei *data breach*

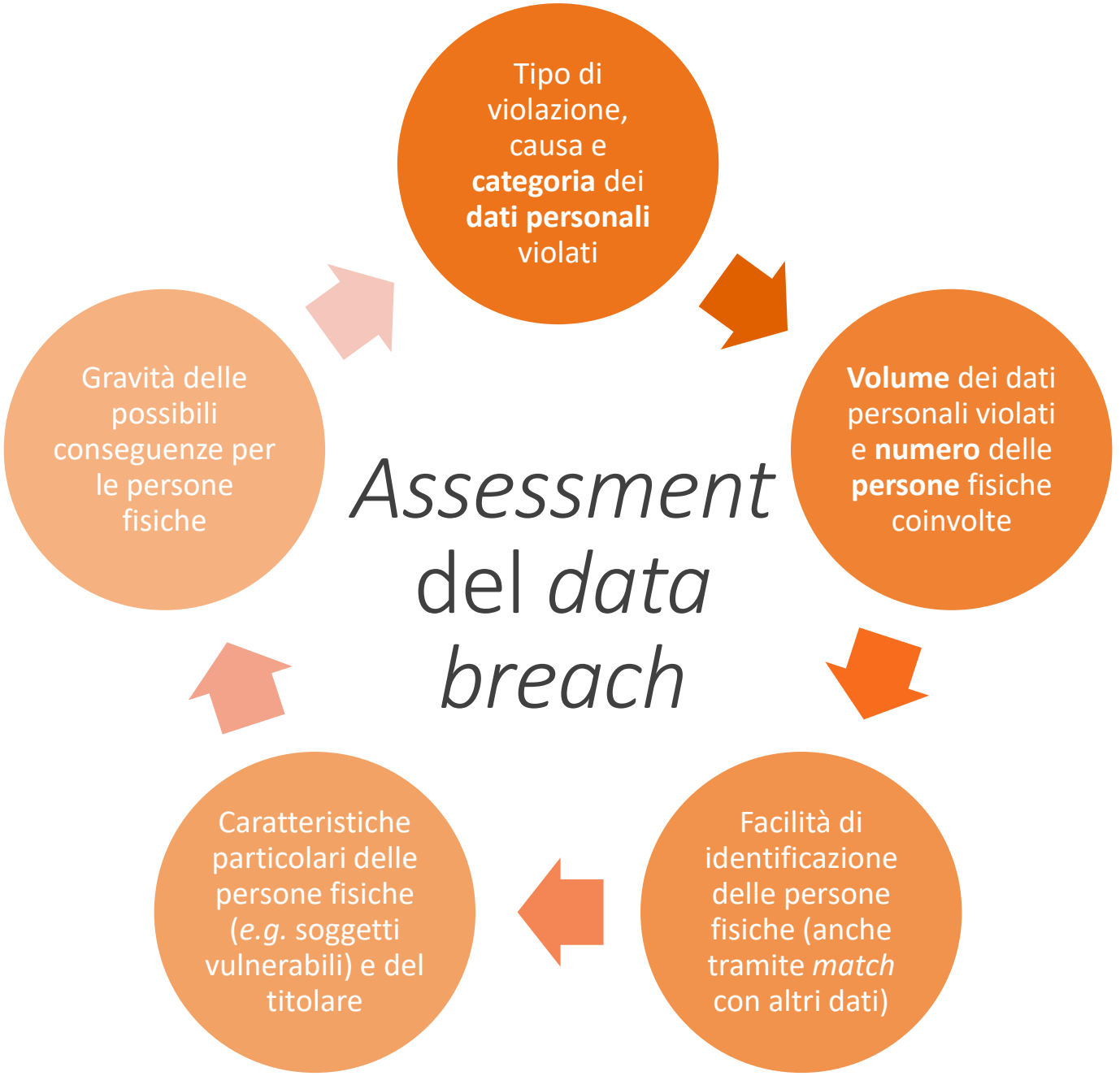
- tipo di violazione
- individuazione criticità e vulnerabilità sfruttate
- identificazione delle aree di miglioramento

Registro dei *data breach* (art. 33, par. 5, GDPR)

- **Dettagli** relativi alla **violazione** (comprese le cause e i fatti)
- Categorie di dati personali oggetti di violazione
- Effetti e **conseguenze** della violazione
- **Provvedimenti** adottati per porvi **rimedio**
- **Ragionamento** alla base delle decisioni prese in risposta a una violazione (*e.g.*, se non si intende procedere a notifica perché si ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche)
- **Motivi dell'eventuale ritardo** nella notifica o nella comunicazione

Cosa fare in caso di *data breach*?




Tipo di violazione, causa e **categoria** dei **dati personali** violati
Volume dei dati personali violati e **numero** delle **persone** fisiche coinvolte
Facilità di identificazione delle persone fisiche (anche tramite *match* con altri dati)
Caratteristiche particolari delle persone fisiche (*e.g.* soggetti vulnerabili) e del titolare
Gravità delle possibili conseguenze per le persone fisiche
Assessment del *data breach*

Notifica all'autorità di controllo (art. 33 GDPR)

*«a meno che sia **improbabile** che la violazione dei dati personali presenti un **rischio** per i diritti e le libertà delle persone fisiche.»*

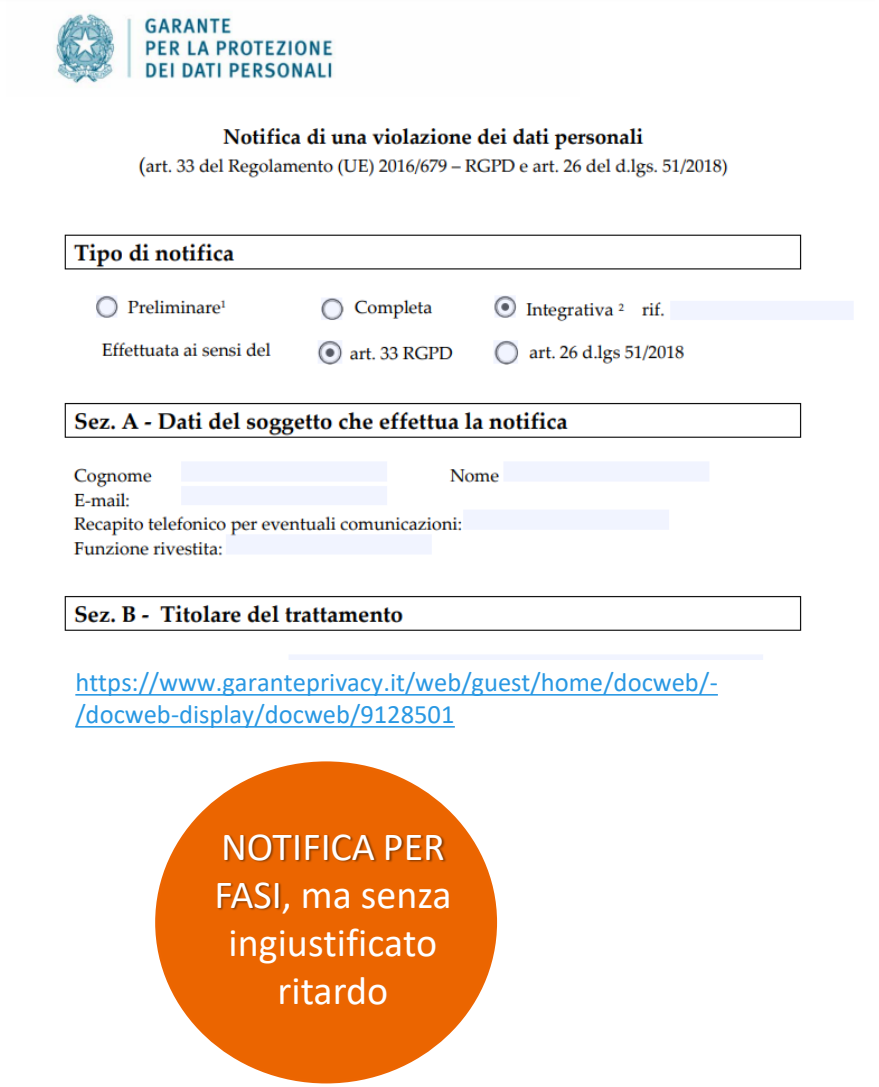
ECCEZIONI

- Violazione avente ad oggetto dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un **rischio probabile** per la persona fisica.
- Violazione avente ad oggetto **dati personali crittografati con un algoritmo all'avanguardia**, a condizione che la riservatezza della chiave rimanga intatta (*i.e.*, non individuabile con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi)... MA

se manca una copia di *backup* dei dati, la loro perdita o l'alterazione possono avere effetti negativi per gli interessati

OBBLIGO DI NOTIFICA

Notifica all'autorità di controllo (art. 33 GDPR)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali
(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501

NOTIFICA PER FASI, ma senza ingiustificato ritardo

Natura della violazione (riservatezza, integrità e disponibilità) dei dati personali

Categorie e il **numero** approssimativo di **interessati** in questione

Categorie e il **numero** approssimativo di **registrazioni** dei dati personali in questione

Nome e i dati di contatto del **DPO** o di **altro punto di contatto** presso cui ottenere più informazioni

Misure adottate o di cui si propone l'adozione **per porre rimedio** alla violazione dei dati personali e anche per attenuarne i possibili effetti negativi

Probabili conseguenze della violazione dei dati personali

Comunicazione agli interessati (art. 34 GDPR)

Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

Comunicazione agli interessati (art. 34 GDPR)

ECCEZIONI (art. 34, par. 3, GDPR)

- il **titolare** del trattamento ha **adottato misure** tecniche e organizzative **adeguate per proteggere i dati personali prima della violazione**, in particolare quelle destinate a **rendere** i **dati personali incomprensibili** a chiunque non sia autorizzato ad accedervi (*e.g.* cifratura o *tokenizzazione*)
- il titolare del trattamento ha **successivamente** adottato **misure** atte a **scongiurare** la concretizzazione di un **rischio elevato** per i diritti e le libertà degli interessati
- la **comunicazione richiederebbe sforzi sproporzionati** (*e.g.* nel caso in cui i dati di contatto siano stati persi o mai resi noti)

MA…

Se l'autorità di controllo ritiene sussistente un elevato rischio alla libertà e ai diritti degli interessati

OBBLIGO DI COMUNICAZIONE

www.lcalex.it

Avv. Gianluca De Cristofaro – gianluca.decristofaro@lcalex.it