ANALISI DEL RISCHIO

IL RISCHIO NEL GDPR

Articolo 32

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**, il **titolare del trattamento** e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**…

2. Nel **valutare l'adeguato livello di sicurezza**, si tiene conto in special modo dei **rischi presentati dal trattamento** che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o dall'**accesso**, in modo **accidentale o illegale**, a dati personali trasmessi, conservati o comunque trattati.

VALUTAZIONE DEL RISCHIO

«…rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche…»

BACINO INTERESSATI (valori annui)	
Descrizione	Valutazione
Da 1 a 20 soggetti	1
Da 21 a 100 soggetti	2
Da 100 a 1.000 soggetti	3
Da 1.001 a 5.000 soggetti	4
Oltre 5.000 soggetti	5

VALUTAZIONE DEL RISCHIO

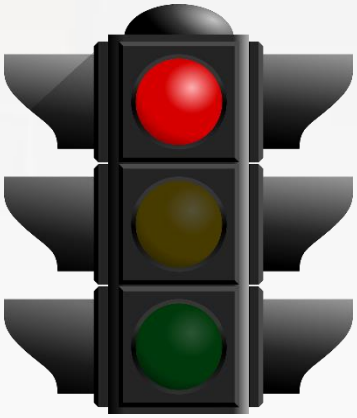
«…rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche…»

TIPOLOGIA DATI	
Descrizione	Val.
Nome, cognome	1
Dati personali (luogo e data di nascita, codice fiscale, grado di parentela / legame familiare)	2
Dati privati (IBAN, Carta Identità, dati di contatto personale, titolo di studio, professione, videoriprese)	3
Dati da cui emerge situazione disagio economico-sociale, dati di minori, info su sanzioni amm.ve	4
Dati sanitari, giudiziari, genetici, particolari, credenziali	5

VALUTAZIONE DEL RISCHIO

«…rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche…»

BACINO DI INTERESSATI X TIPOLOGIA DI DATI ≥ 15



VALUTAZIONE DEL RISCHIO

*«… **rischi presentati dal trattamento** che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o dall'**accesso**, in modo **accidentale o illegale**…»*

CODICE	DESCRIZIONE DEL RUOLO DELL'UFFICIO NEL TRATTAMENTO	RISERV	INTEGR	DISPON
RIFER	Ufficio di riferimento del trattamento. Fa capo a tutte le azioni previste per il trattamento dei dati, dalla raccolta alla conservazione e/o cancellazione del dato	SI	SI	SI
CONSULT	Consultazione (senza possibilità di modifica) del dato strumentale ad altre finalità proprie dell'ufficio che effettua il trattamento	SI	NO	NO
SUPP	Attività di supporto all'ufficio di riferimento con integrazione dei dati e delle informazioni relative al trattamento (senza possibilità di modifica e/o cancellazione delle informazioni primarie)	SI	SI	NO
STRUM	Attività strumentali alle finalità perseguite dall'ufficio di riferimento, su sua specifica disposizione (senza la possibilità modifica e/o cancellazione dei dati primari), per lo svolgimento di funzioni specifiche correlate al procedimento	SI	NO	NO
COLLAB	Attività di collaborazione con l'ufficio di riferimento nel trattamento dei dati, che comportano operazioni di raccolta, modifica, integrazione, cancellazione di dati primari	SI	SI	SI
CUST	Attività di custodia dei dati o di copia dei dati in formato informatico o cartaceo	SI	NO	SI
ADS	Attività di amministrazione di sistema sull'ambito applicativo utilizzato nel trattamento di dati	SI	SI	SI

TRATTAMENTI RISCHIOSI

se BACINO DI INTERESSATI X TIPOLOGIA DI DATI ≥ 15

→ Analisi delle risorse coinvolte

(Office automation, Posta elettronica, Applicativi specifici)

TRATTAMENTI RISCHIOSI

se BACINO DI INTERESSATI X TIPOLOGIA DI DATI ≥ 15

→ Analisi delle risorse coinvolte (perimetri)

(Office automation, Posta elettronica, Applicativi specifici)

RISORSE COINVOLTE

PERIMETRO TECNOLOGICO	APPLICATIVO GESTIONE PROTOCOLLO INFORMATICO
SOFTWARE	Nome SW e fornitore
TIPOLOGIA APPLICATIVO	[A] Client/Server su PC [B] Client/Server su server [C] Applicazione Web Interna
GESTIONE DELLE UTENZE	Descrizione breve procedure autorizzative di rilascio utenze (email, ticket, registri/elenchi utenti anche informatici)
TIPOLOGIE HW DELLA COMPONENTE SERVER [A] [B] [C]	Età server fisico che ospita l'applicazione: Server virtualizzato: SI/NO Server sotto manutenzione: SI/NO Ridondanze: (RAID, Alimentazione, Cluster…) Gruppo di continuità/gruppo elettrogeno: SI/NO Aggiornamenti dei sistemi: (Ultimo anno, da 1 a 3 anni, > 3 anni)
SISTEMI DI BACKUP [A] [B] [C]	Tipologia di backup: (copia degli archivi, delle macchine virtuali, backup a caldo, backup a freddo…) Disponibili supporti di backup offline: SI/NO Sistema di backup residente su altra rete logica: SI/NO Localizzazione supporti di backup; (presso le stessa sede del server, presso una seconda sede dell'ente, in cloud…) Test di ripristino: SI/NO (nel primo caso specificare l'esito)

RISORSE COINVOLTE

PERIMETRO TECNOLOGICO	APPLICATIVO GESTIONE PROTOCOLLO INFORMATICO
NOME SW E FORNITORE	Nome SW e fornitore
TIPOLOGIA APPLICATIVO	[D] Applicazione Web Esterna (hosting o cloud)
GESTIONE DELLE UTENZE	Descrizione breve procedure autorizzative di rilascio utenze (email, ticket, registri/elenchi utenti anche informatici)
FORNITORE SOLUZIONE REMOTA [D]	Nome fornitore
LOCALIZZAZIONE ARCHIVI [D]	ITALIA / EUROPA /EXTRA UE
DESIGNAZIONE RESPONSABILE [D]	SI/NO
MISURE MINIME ADOTTATE	SI/NO

RISCHI DA VALUTARE (AMBIENTALI)

Impossibilità di accesso ai locali
Blackout
Mancanza o sbalzi di energia elettrica
Esondazione/Inondazione
Incendio
Valori estremi di temperatura e umidità
Terremoto

RISCHI DA VALUTARE (UMANI)

Accesso non autorizzato alla risorsa
Assenza di personale “chiave” ovvero di personale indispensabile per la corretta erogazione dei servizi
Dolosa Cancellazione / Modifica / Distruzione non autorizzata di dati o documenti
Errata Cancellazione / Modifica / Distruzione involontaria di dati e/o documenti
Errori imputabili a terzi, in servizi gestiti in outsourcing (ovvero gestiti da personale esterno all’amministrazione)
Errori umani nella gestione della sicurezza
Appropriazione indebita di informazioni protette

RISCHI DA VALUTARE (UMANI)

Furto degli strumenti
Manomissione e/o sabotaggio
Smarrimento della risorsa
Sottrazione di credenziali di autenticazione
Uso di “software pirata” (software privo di relativa licenza e scaricato, per esempio, da internet con i relativi aggiornamenti)
Trattamento dei dati eccedente le finalità
Utilizzo non autorizzato della risorsa

RISCHI DA VALUTARE (TECNOLOGICI)

Impossibilità di accesso alla risorsa
Errori imputabili al software
Guasto di apparati e/o impianti accessori
Malfunzionamenti della risorsa
Malware
Phishing
Ransomware
Spam
Attacchi web based

IL PIANO DEI TRATTAMENTI

Descrizione degli interventi proposti per mitigare i rischi rilevati sulle varie risorse, con tempi e modalità

Definizione del Piano di trattamento				
Azioni definite			Risultati	
N°	Proposta azione	Aree coinvolte	Termine previsto	Esito
1	Regolamento di utilizzo delle risorse informatiche	Servizio Informativo, tutti gli uffici		
2	Formazione al personale sul regolamento e sulle basi della protezione dei dati personali	Servizio Informativo, tutti gli uffici		
3	Strutturazione dei processi di rilascio credenziali di accesso alle informazioni e strumentazione informatica	Servizio Informativo, tutti gli uffici		

RISCHI E INCIDENTI

RGPD

REGOLAMENTO (UE) 2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dei primi 4 mesi di applicazione

Un primo bilancio sull'applicazione in Italia, a partire dal 25 maggio, del **Regolamento europeo in materia di protezione dei dati personali** mostra come pubbliche amministrazioni, mondo delle imprese e cittadini abbiano colto l'importanza del nuovo quadro giuridico e le opportunità che esso offre in termini di tutela e garanzie per le persone.

Comunicazioni dei dati di contatto degli RPD

40.738

Reclami e segnalazioni

2.547

(1.795 nello stesso periodo 2017)

Notificazioni di Data Breach

305

Contatti con l'URP

circa 7.200

(circa 4.400 nello stesso periodo 2017)

Dati aggiornati al 28 settembre 2018

www.garanteprivacy.it

DATA BREACH E'…

DATA BREACH

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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 di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

DATA BREACH

SI.NET Servizi Informatici

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento**.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

SCENARI: DISTRUZIONE

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, **non è più nella disponibilità del titolare**, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.

SCENARI: PERDITA

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, **non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente)**. In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.

SCENARI: MODIFICA

Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato **irreversibilmente modificato, senza possibilità di ripristinare lo stato originale**. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.

SCENARI: DIVULGAZIONE NON AUTORIZZATA

Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene **trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione**.

SCENARI: ACCESSO NON AUTORIZZ.

Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi **disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza**, o secondo i regolamenti dell'organizzazione.

SCENARI: INDISPONIBILITA' TEMPORANEA DEL DATO

Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è **non disponibile per un periodo di tempo che lede i diritti dell'interessato**.

WP29 - CASO 1

Un titolare ha fatto un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.

WP29 - CASO 1

Un titolare ha fatto un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.

Notifica all'Autorità di Controllo: NO

Notifica all'interessato: NO

WP29 - CASO 2

Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati.

WP29 - CASO 2

Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati.

Notifica all'Autorità di Controllo: SI, riferire all'autorità di vigilanza se vi sono probabili conseguenze per le persone.

Notifica all'interessato: SI, riferire alle persone a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per gli individui è elevata.

WP29 - CASO 3

Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare comporta che i clienti non siano in grado di chiamare il titolare e accedere ai loro record.

WP29 - CASO 3

Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare comporta che i clienti non siano in grado di chiamare il titolare e accedere ai loro record.

Notifica all'Autorità di Controllo: NO

Notifica all'interessato: NO

WP29 - CASO 4

Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, emerge che l'unica funzionalità del ransomware sia quella di crittografare i dati e che non vi erano altri malware presenti nel sistema.

WP29 - CASO 4

Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, emerge che l'unica funzionalità del ransomware sia quella di crittografare i dati e che non vi erano altri malware presenti nel sistema.

Notifica all'Autorità di Controllo: SI, riferire all'autorità di vigilanza, se ci sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.
Notifica all'interessato: SI, riferire ai singoli, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.

WP29 - CASO 5

Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile per qualcun altro.
Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ha un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.

WP29 - CASO 5

Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile per qualcun altro.
Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ha un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.

Notifica all'Autorità di Controllo: SI
Notifica all'interessato: Solo le persone colpite vengono avvisate se c'è un rischio elevato ed è ragionevolmente certo che altri soggetti non siano stati colpiti.

WP29 - CASO 6

Un titolare gestisce un sito di e-commerce ed ha clienti in più Stati membri. Il sito subisce un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.

WP29 - CASO 6

Un titolare gestisce un sito di e-commerce ed ha clienti in più Stati membri. Il sito subisce un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.

Notifica all’Autorità di Controllo: SI, segnalare all'autorità di vigilanza principale se il trattamento è transfrontaliero.

Notifica all’interessato: SI, in quanto potrebbe comportare alto rischio.

WP29 - CASO 7

Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico.

WP29 - CASO 7

Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico.

Notifica all'Autorità di Controllo: SI, l'ospedale è obbligato a notificare la violazione come ad alto rischio per il benessere del paziente e per la sua privacy.

Notifica all'interessato: SI, occorre riferire alle persone colpite.

WP29 - CASO 8

I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.

WP29 - CASO 8

I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.

Notifica all'Autorità di Controllo: SI, occorre riferire all'Autorità di Vigilanza.

Notifica all'interessato: SI, riferire alle persone in base alla portata e al tipo di dati personali coinvolti, oltre che alla gravità delle possibili conseguenze.

WP29 - CASO 9

Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.

WP29 - CASO 9

Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.

Notifica all'Autorità di Controllo: SI, la notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene le password iniziali).
Notifica all'interessato: SI, occorre riferire alle persone in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.

COSA FARE IN CASO DI INCIDENTE

In caso di incidente è necessario contattare immediatamente il Responsabile Protezione Dati, al fine di analizzare la tipologia di incidente e stabilire se è un data breach da segnalare al Garante della Privacy (ed eventualmente agli interessati)

Grazie per l'attenzione

aldo.lupi@sinetinformatica.it

Per seguire l'innovazione nella PA:

www.sinetinformatica.it

www.sinetinformatica.it/twitter

www.sinetinformatica.it/facebook