



UNIVERSITÀ  
POLITECNICA  
DELLE MARCHE

DII

Dipartimento di Ingegneria  
dell'Informazione



unIMC

# Gestione e Prevenzione dei *Data Breaches*: Caso pratico in Ente Locale

Donatella Bruni

Venerdì 3 Ottobre 2025



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

# Agenda dei Contenuti

---

**01** L'idea sottesa al concetto di *data breach*: la violazione della privacy

**02** GDPR: indicazioni normative, *severity calculator*

**03** Il portale del Garante Privacy

**04** Focus: strategie di prevenzione dei Data Breaches e gestione della privacy in Regione Calabria



---

# 01 L'idea sottesa al concetto di *Data Breach*: la violazione della privacy



# 01. Violazione privacy



# Violazione Privacy



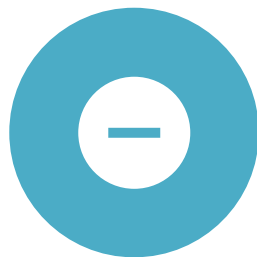
VIOLATA LA  
RISERVATEZZA DEI DATI  
PERSONALI



TRATTAMENTO ILLECITO  
DEI DATI



RESPONSABILITÀ CIVILE



DIFFUSIONE ILLECITA DI  
DATI PERSONALI



DOXING

# Data Breach



VIOLAZIONE DEI DATI  
PERSONALI



ELEMENTO "RISCHIO"



TRATTAMENTO  
ILLECITO DEI DATI



RESPONSABILITÀ  
CIVILE E PENALE



DIFFUSIONE ILLECITA  
DI DATI PERSONALI



ONERE DI VERIFICA



OBBLIGO DI NOTIFICA  
ENTRO 72 ORE

---

## 02 GDPR: indicazioni normative, *Severity Calculator*



## 02. GDPR: Indicazioni Normative, *Severity Calculator*



- Decreto Legislativo 30 giugno 2003, n. 196
- Regolamento (UE) 2016/679 (GDPR) [artt. 32-34]
- Decreto Legislativo 10 agosto 2018, n. 101
- ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013
- EPDB, Guidelines 9/2022 on personal data breach notification under GDPR



# I profili della violazione

- R – violazione della riservatezza
- I – violazione dell'integrità
- D – violazione della disponibilità



# Severity Calculator

- Valutazione del rischio derivante dal *Data Breach*
- GDPR individua 3 tipologie di rischio
  - Rischio gestibile a livello di accountability, privacy by design, privacy by default;
  - Rischio residuo;
  - Rischio specifico ricadente a seguito di data breach
- Formula alla base del Severity Calculator

$$SE = DPC \times EI + CB$$



# Valutazione d'Impatto (DPIA)

- Valutazione d'impatto sulla protezione dei dati
- Da condurre *prima* di procedere al trattamento dei dati
- Obbligatoria in alcuni casi:
  - Trattamenti valutativi
  - Decisioni automatizzate con effetti giuridici
  - Monitoraggio sistematico
  - Dati sensibili
  - Trattamenti dati su larga scala
  - Creazione di corrispondenze
  - Trattamento dati soggetti vulnerabili
  - Nuove soluzioni tecnologiche

# Qualche numero (Relazione Garante Privacy 2024)



2.204 DATA BREACHES  
SEGNALATI



835 PROVVEDIMENTI  
ADOTTATI DAL GARANTE



24 MILIONI DI EURO DI  
SANZIONI IRROGATE



130 ISPEZIONI  
CONDOTTE

---

## 03 Il portale del Garante Privacy



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

# Il portale del Garante Privacy

<https://servizi.gpdp.it/>



Garante per la protezione dei dati personali



## Notifica di una violazione dei dati personali (data breach)

art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs. 51/2018

Auto valutazione per la notifica di una violazione dei dati personali (data breach)



Compilazione della notifica



Istruzioni



Informativa sul trattamento dei dati personali



Pagina informativa - Violazione dei dati personali (data breach)



Fac-simile del modello



# Il portale del Garante Privacy

<https://servizi.gpdp.it/>



NOTIFICA DATA BREACH

10% COMPLETATO

## B) Tipo di notifica

**i** In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (Prima notifica). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (Notifica integrativa) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

### Prima notifica

- a) Completa
- b) Preliminare<sup>1</sup>

### La notifica viene effettuata

- ai sensi dell'art. 33 RGPD
- ai sensi dell'art. 26 d.lgs 51/2018

### Notifica integrativa<sup>2</sup>

- c) fascicolo

n.

?

PIN

?

<sup>1</sup> Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per fornire le informazioni di cui non è ancora in possesso.

<sup>2</sup> Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33, par. 4, del Regolamento, integra una precedente notifica.

Indietro

Avanti

# Il portale del Garante Privacy

<https://servizi.gpdp.it/>



## C) Titolare del trattamento

### 1) Il Titolare del trattamento è:

**i** Indicare l'eventuale registro all'interno del quale è censito il titolare del trattamento che effettua la notifica. A tal fine si rappresenta che tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad ordini o collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC, cfr. DL 29 novembre 2008 n.185 e DL 19 ottobre 2012, n. 179). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

- Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti  
(INI-PEC [www.injpec.gov.it](http://www.injpec.gov.it) - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)
- Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (Tipologie Enti: Pubbliche Amministrazioni)  
(IPA [www.indicepa.gov.it](http://www.indicepa.gov.it) - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)
- Non censito in nessuno dei due precedenti indici

### 2) Dati del Titolare del trattamento:

**i** Indicare le informazioni relative al titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione

Codice Fiscale

Stato

Provincia

CAP

Indirizzo

Comune

Telefono

# Il portale del Garante Privacy

<https://servizi.gpdp.it/>



L'Autorità ▼ Temi ▼ Normativa e provvedimenti ▼ News e comunicazione ▼ Amministrazione Trasparente



## FINALMENTE UN PO' DI PRIVACY

Campagna di comunicazione istituzionale finalizzata a promuovere i temi della protezione dei dati, della privacy e dell'educazione digitale

Diffondere il valore dei dati e l'importanza di proteggerli, raccontando il lavoro di un'Autorità vicina alla gente.

È questo l'obiettivo della campagna di comunicazione istituzionale, intitolata **"Finalmente un po' di privacy"**, che segue una narrazione in cui il Garante, impersonato da un attore, interviene in diverse situazioni quotidiane in aiuto alle persone che vedono insidiata la propria privacy e i propri dati personali.

Dall'uso delle app alle frodi digitali, dal cyberbullismo al revenge porn, dal telemarketing selvaggio agli assistenti digitali, dai dati sanitari alla profilazione e all'uso delle password, il Garante è sempre pronto a mettere in guardia dai rischi di un uso improprio dei dati e a indicare le forme di tutela.

Il claim finale **"Se proteggi i tuoi dati proteggi stesso"** è un invito ad essere sempre più consapevoli del "valore privacy".

La campagna è stata finanziata dal **Ministero delle Imprese e del Made in Italy** con il fondo a vantaggio dei consumatori.

Agli spot si sono affiancate anche **affissioni digitali** visibili negli aeroporti di Torino Caselle, Milano Linate, Napoli Capodichino. Le stesse affissioni sono state inoltre ospitate, a titolo gratuito, da Ferrovie dello Stato Italiane sulle Frecce e sui nuovi treni

### Temi

- Banche, credito, finanza ▼
- Biometria
- Creative Commons
- Cyberbullismo
- Cybersecurity ▼
- Fisco ▼
- Giornalismo ▼
- Informazioni commerciali
- Iniziative formative ▼
- AI - Intelligenza artificiale ▲

AI - Intelligenza artificiale

Assistenti digitali (Smart Assistant)

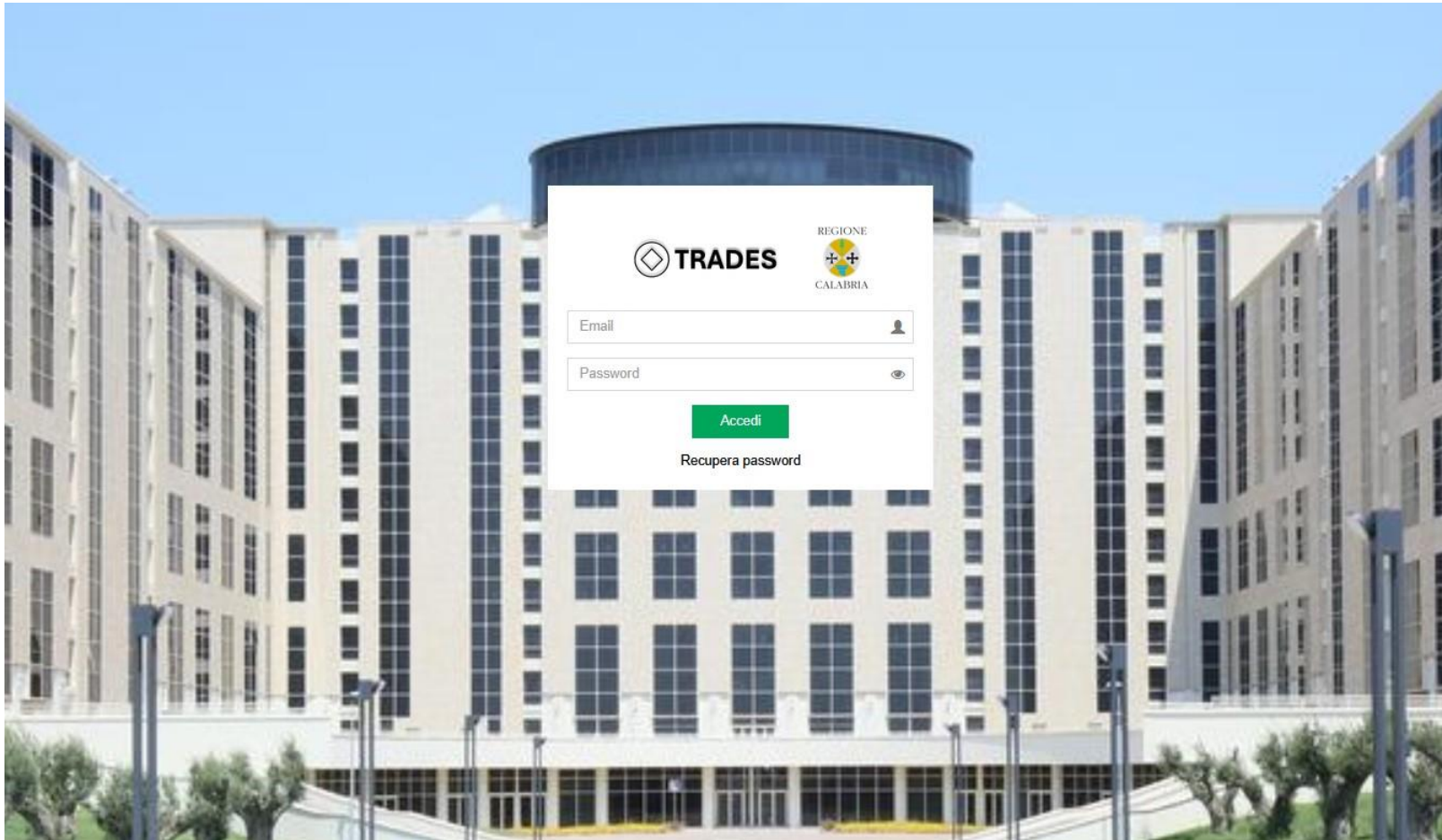
Deepfake

---

## 04 Focus: strategie di prevenzione dei Data Breaches e gestione della Privacy in Regione Calabria



## 03. Focus Regione Calabria



## 03. Focus Regione Calabria - Formazione



### MONITORAGGIO NORMATIVO PRIVACY

Monitoraggio normativo Privacy | Luglio 2025

#### ULTIME NOTIZIE DAL MONDO PRIVACY

Gentilissimi,  
vogliamo condividere con voi le ultime notizie e i provvedimenti più significativi che riguardano il mondo Privacy. In un'epoca in cui la protezione dei dati personali è di cruciale importanza, è fondamentale rimanere costantemente aggiornati sulle ultime tendenze per affrontare con successo le sfide legate alla protezione dei dati e al loro uso responsabile. Di seguito un estratto delle notizie.

Buona lettura!



# 03. Focus Regione Calabria - Applicativo



**TRADES** **FASE 1** Privacy by design **FASE 2** Valutazioni di impatto **FASE 3** Registro trattamenti **FASE 4** Verifiche periodiche **FASE 5** Gestione interessati **FASE 6** Gestione incidenti **FASE 7** Privacy dashboard **Altre risorse (link utili)** **DB**

Registro regionale delle attività di trattamento del Titolare del Trattamento (art. 30, par. 1 del GDPR)

Dati estratti [excel](#) [csv](#) [Q](#) [filtra](#) [+ aggiungi trattamento](#)

#	codice	stato	macro-ambito organizzativo	ambito del trattamento	denominazione del trattamento	finalità del trattamento (ex art.30 GDPR)	categorie di dati personali (ex art.30 GDPR)	categorie di interessati (ex art.30 GDPR)	categorie di destinatari (ex art.30 GDPR)
1	28257	In corso			Gestione del personale	GESTIONE DEL PERSONALE – AFFARI GENERALI + ADEMPIMENTI IN MATERIA DI PRIVACY...	dati di identificazione personale, dati su vita o stato di salute o orientamento sessuale,...	dipendenti	strutture interne all'ente, enti pubblici
2	28264	In corso			Gestione della corrispondenza	GESTIONE CORRISPONDENZA	dati su occupazione lavorativa, dati di contatto, dati economici o finanziari o fiscali, d...	dipendenti, personale di enti/società privati, personale di enti pubblici	strutture interne all'ente, enti pubblici
3	28268	In corso			Pubblicazione decreti sul portale Trasparenza Regcal e relat..	ADEMPIMENTI CONNESSI AL PROCEDIMENTO AMMINISTRATIVO	dati di identificazione personale, dati su occupazione lavorativa, dati di contatto, dati ...	cittadini, collaboratori/professionisti esterni, iscritti in albi ed elenchi, candidati po...	privati, enti pubblici
4	28269	In corso			Gestione del protocollo	Gestione protocollo	dati di identificazione personale, dati su occupazione lavorativa, dati di contatto, dati ...	dipendenti, personale di enti/società privati, cittadini, iscritti in albi ed elenchi, can...	privati, strutture interne all'ente, organi di vigilanza e controllo, autorità giudiziaria...

# 03. Focus Regione Calabria - Applicativo



Altre risorse  
(link utili)

DB

## Pre-valutazione DPIA (PDPIA)

Dati estratti excel csv Q filtra

#	trattamento	stato	DPIA	macro-ambito organizzativo	ambito di trattamento dei dati	data
1	28268. Pubblicazione decreti sul portale Trasparenza Regcal e relativo monitoraggio	DPIA non prevista				
2	28269. Gestione del protocollo	DPIA non prevista				
3	28257. Gestione del personale	DPIA non prevista				
4	28264. Gestione della corrispondenza	DPIA non prevista				

Record 4 - Pagine 1

# 03. Focus Regione Calabria - Applicativo



TRADES

FASE 1 Privacy by design

FASE 2 Valutazioni di impatto

FASE 3 Registro trattamenti

FASE 4 Verifiche periodiche

FASE 5 Gestione interessati

FASE 6 Gestione incidenti

FASE 7 Privacy dashboard

Altre risorse (link utili)

DB

## Gestione verifiche (VTRATT)

Dati estratti excel csv Q filtra

+ inserisci analisi VTRATT

#	Trattamento	Autore	Macroambito	Ambito	Creato	Modificato	Stato	Dashboard
1	28268. Pubblicazione decreti sul portale Trasparenza Regcal e relativo monitoraggio						completato	
2	28264. Gestione della corrispondenza						completato	
3	28269. Gestione del protocollo						completato	
4	28257. Gestione del personale						completato	

# 03. Focus Regione Calabria - Applicativo



Trattamento del Titolare

Inserisci i seguenti dati

**?** denominazione del trattamento \*

**?** descrizione delle attività di trattamento

**?** stato del trattamento

In corso

**?** finalità del trattamento (ex art.30 GDPR)

---

**?** base giuridica per il trattamento

---

**?** base giuridica per il trattamento di categorie particolari di dati personali o di dati personali giudiziari

---

**?** categorie di dati personali (ex art.30 GDPR)

Aggiungi

**?** categorie di interessati (ex art.30 GDPR)

Aggiungi

**?** categorie di destinatari (ex art.30 GDPR)

Aggiungi

**?** contitolari (ex art.30 GDPR, ove applicabile)

# 03. Focus Regione Calabria - Applicativo



Gestione verifiche (VTRATT)

Inserisci i seguenti dati

**? trattamento \***

Modifica Elimina

**? Iniziativa \***

---

**? Stato \***

in bozza

**? Note**

Sezione 1 - Capacità di individuare e qualificare i dati personali trattati

1 Esaminando i dati personali, ha valutato l'eventuale presenza di dati appartenenti a minori (art. 8 del GDPR) o a "categorie particolari di dati personali" (art. 9 del GDPR)? ---

2 Ha valutato anche l'eventuale presenza di dati personali relativi a condanne penali e reati (art. 10 del GDPR)? ---

Sezione 2 - Percezione delle responsabilità in capo ai Delegati del Titolare

3 E' a conoscenza del Regolamento regionale n. 20 del 18 dicembre 2018 per come modificato dalla DGR n.29 del 1 febbraio 2021 recante "Attribuzione delle competenze in materia di trattamento dei dati personali nell'ambito delle strutture organizzative della Giunta regionale" ---

4 Sono state determinate le finalità del trattamento dei dati personali? ---

5 Sono state determinate le modalità del trattamento dei dati personali? ---



**Grazie per l'attenzione!**