

Documento	REGISTRO VIOLAZIONI INFORMATICHE
Classe / tipologia	Registro / Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "DATA BREACH" 2/7/2015 - Artt. 32 e 33 REG.679/16
Documenti relati	INDEX679, SOP3_3, DT679, IO-DB01, DVR/IP, DP-PG679
Riferimenti	Piano di adeguamento 2023-24

#### CONTENUTI

- ISTRUZIONI USO E COMPILAZIONE
- MODULO REGISTRAZIONE VIOLAZIONE "Data Breach"

La politica gestionale del documento DB-PG679 e la relativa Istruzione Operativa IO-DB01 prevedono che in merito alla gestione degli incidenti informatici aziendali e più in particolare per ciò che attiene le violazioni di cui al provvedimento c.d. "Data Breach" venga detenuto un REGISTRO DELLE VIOLAZIONI (RV-DB01)

Questo documento compendia i due riferimenti di cui sopra e viene preso in carica dal GDR-IT sotto controfirmato

#### ISTRUZIONE D'USO E COMPILAZIONE

La registrazione di un evento di violazione viene registrata nel modulo annesso al presente documento. Ogni modulo identifica un sintetico rapporto descrittivo associato alle seguenti informazioni base:

- *Nome operatore del GDR-IT*
- *Data e ora dell'evento avverso*
- *Descrizione evento*
- *Valutazione danno/gravità presunta*
- *Valutazione danno/gravità definitiva*
- *Descrizione delle attività di risposta*
- *Estremi documentazione e/o fascicolo attività di risposta*
- *Conclusioni ufficiali del TDT*

Il modulo RV-DB01 opportunamente compilato viene firmato stampato e acquisito in copia digitale per essere pubblicato sul MSPPD del sito INTRALAN aziendale (se presente).

<input type="checkbox"/>	TITOLARE	.....
<input type="checkbox"/>	RESPONSABILE	.....
<input type="checkbox"/>	GRUPPO RISPOSTA	.....
<input type="checkbox"/>	ADS / DBA	.....



## REGISTRO DELLE VIOLAZIONI INFORMATICHE

REGISTRO VIOLAZIONI INFORMATICHE  
 PROV. "DATA BREACH" 2/7/2015 - Artt. 32 e 33 REG.679/16  
 INDEX679, SOP3\_3, DT679, IO-DB01, DVR/IP, DP-PG679  
 Piano di adeguamento 2023-24

**MODULO DI RILEVAMENTO**

Data:.....	Operatore: .....	Ore: .....
DESCRIZIONE INIZIALE EVENTO: .....		
.....		
.....		
VALUTAZIONE DANNO / GRAVITA' PRESUNTA : ..... / .....		
VALUTAZIONE DANNO / GRAVITA' RILEVATA : ..... / .....		
DESCRIZIONE ATTIVITA' DI RISPOSTA: .....		
.....		
.....		
ESTREMI DOCUMENTAZIONE / FASCICOLI ATTIVITA' DI RISPOSTA :.....		
.....		
.....		
CONCLUSIONI UFFICIALI DEL TDT:.....		
.....		
.....		

- TITOLARE .....
- RESPONSABILE .....
- GRUPPO RISPOSTA .....
- ADS / DBA .....

SPPD

Framework



**REGISTRO VIOLAZIONI INFORMATICHE**  
**PROVV. "DATA BREACH" 2/7/2015 - Artt. 32 e 33 REG.679/16**  
**INDEX679, SOP3\_3, DT679, IO-DB01, DVR/IP, DP-PG679**  
 Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

**S E G N A L A Z I O N E / V I O L A Z I O N E**

**Codice evento:** ..... **Segnalante:** ..... **Unità organizzativa:** .....

**FUNZIONE INFORMATATA:** .....

**LUOGO VIOLAZIONE:** .....

**MODALITA' VIOLAZIONE** (*flusso dei dati*)

.....  
 .....

**TARGET DELLA VIOLAZIONE** (*Sistemi/reti/apparati o Banche Dati*)

.....  
 .....

**NATURA DELLA VIOLAZIONE** (*riservatezza, integrità e/o disponibilità dei dati*)

.....  
 .....

**ALTRI ELEMENTI VIOLAZIONE** (*circostanze utili di contesto*)

.....  
 .....

REGISTRO VIOLAZIONI INFORMATICHE  
PROVV. "DATA BREACH" 2/7/2015 - Artt. 32 e 33 REG.679/16  
INDEX679, SOP3\_3, DT679, IO-DB01, DVR/IP, DP-PG679  
Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

## DATI-INTERESSATI / CONSEGUENZE / MITIGAZIONE

CATEGORIA INTERESSATI	NUMERO INTERESSATI	CATEGORIA DATI
-----------------------	--------------------	----------------

.....

NUMERO DI DATI INTERESSATI : .....

TIPOLOGIA DELLE CONSEGUENZE (*danni di pregiudizio, materiali, patrimoniali o reputazionali*)

.....  
.....

CONTROMISURE **REMEDIAZIONE** (*Precauzioni già in essere che compensano le conseguenze*)

.....  
.....

**REMEDIAZIONE** ADDIZIONALI (*Precauzioni che si intende adottare o in corso di adozione*)

.....  
.....

CONTROMISURE **MITIGAZIONE** (*Precauzioni attenuano e/o mitigano le conseguenze*)

.....  
.....

**MITIGAZIONE** ADDIZIONALI (*Precauzioni attenuano e/o mitigano le conseguenze*)

.....  
.....

REGISTRO VIOLAZIONI INFORMATICHE  
PROVV. "DATA BREACH" 2/7/2015 - Artt. 32 e 33 REG.679/16  
INDEX679, SOP3\_3, DT679, IO-DB01, DVR/IP, DP-PG679  
Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

## TEMPISTICHE / NOTIFICHE AC/ COMUNICAZIONI

TEMPI DURATA STIMATA	TEMPI RIPRISTINO	TEMPI RECUPERO
----------------------	------------------	----------------

.....

**RISCHIO PER DIRITTI E LIBERTA' DI PERSONE FISICHE:** ..... (Probabile/Non Probabile)

*Nota alla compilazione:* considerare 1) Tipo di violazione; 2) Natura, carattere sensibile e volume dei dati personali; 3) Facilità di identificazione delle persone fisiche; 4) Gravità delle conseguenze per le persone fisiche; 5) Caratteristiche particolari dell'interessato; 6) Caratteristiche particolari del titolare del trattamento di dati; 7) Numero di persone fisiche interessate; 8) Aspetti generali.

**INVIO NOTIFICAZIONE INCIDENTE ALLA AUTORITA' DI CONTROLLO:** .....

.....  
.....

*Nota alla compilazione:* indicare sì/no; in caso affermativo indicare data e ora; se totale o parziale; in tale caso, il numero ordinale della notifica (prima, seconda, ecc.) o se ultima

**DESCRIZIONE / MOTIVAZIONI DI UNA NOTIFICAZIONE PARZIALE:** .....

.....  
.....

*Note alla compilazione:* ad esempio necessità di effettuare ulteriori indagini; se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'Autorità di Controllo. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

**DESCRIZIONE / MOTIVAZIONI DI RITARDO DI NOTIFICAZIONE:** .....

.....  
.....

*Note alla compilazione:* indicare circostanze relative all'accertamento della violazione che giustifichino il ritardo posteriore a 72 ore. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo.

DESCRIZIONE / MOTIVAZIONI DI OMESSA NOTIFICA: .....

.....  
.....

*Nota alla compilazione:* ad esempio dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica; dati personali resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup; dati personali correttamente crittografati

INDICARE SE RICORRE UN ELEVATO RISCHIO: .....

.....  
.....

INVIO COMUNICAZIONE AGLI INTERESSATI: .....

.....  
.....

*Nota alla compilazione:* indicare sì/no; in caso affermativo indicare data e ora; indicare se effettuata su ordine della Autorità di Controllo

MODALITA' DELLA COMUNICAZIONE AGLI INTERESSATI: .....

.....  
.....

*Nota alla compilazione:* si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard; esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituisce un mezzo efficace. A seconda delle circostanze, utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto. usare formati alternativi appropriati e lingue pertinenti

MOTIVAZIONI DI OMESSA COMUNICAZIONE AGLI INTERESSATI: .....

.....  
.....

*Nota alla compilazione:* inserire una delle ipotesi di cui all'art. 34, par. 3, lett. a), b), c) Gdpr. ad esempio, a seconda dei casi: cifratura allo stato dell'arte oppure mediante tokenizzazione; immediata individuazione e avvio di un'azione contro il soggetto che ha avuto accesso ai dati personali prima dell'utilizzo; comunicazione pubblica o prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta