*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

# Procedura Privacy Nr P04

# GESTIONE DI DATA BREACH AI SENSI DEL GDPR (REGOLAMENTO EUROPEO 679/2016)

**Pubblicazione:** l'ultima revisione del presente documento protocollato e in formato pdf è disponibile per i **destinatari** nei seguenti archivi:

1. Archivio del protocollo ufficiale;
2. Amministrazione trasparente, sez. privacy; agli atti.

### *Tabella degli Indici delle revisioni*

| Prot. n° | Modifiche rispetto alla revisione precedente | Data |
|---|---|---|
| 1215 | Prima emissione | 10/02/2025 |
| | | |
| | | |

**Nota:** in caso di revisione della procedura le modifiche attuate saranno evidenziate in giallo nel corpo del documento.

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

**INDICE:**

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

## 1. SCOPO

Il presente documento si prefigge lo scopo di definire le opportune modalità di gestione del **data breach**, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel **Regolamento UE 679/2016**.

## 2. VALIDITÀ

Il presente documento ha validità all'interno della presente Istituzione scolastica.

## 3. RIFERIMENTI NORMATIVI

| Rif. | CODICE | OGGETTO |
|---|---|---|
| [1] | **D.lgs. n.101/2018** | Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 |
| [2] | **REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Consiglio, del 27 aprile 2016** | Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). |
| [3] | **Provvedimento del Garante del 30 luglio 2019** | Sulla notifica delle violazioni dei dati personali (doc. web n. 9126951) |
| [4] | **ENISA - European Union Agency for Network and Information Security Working Document, v1.0, December 2013** | Recommendations for a methodology of the assessment of severity of personal data breaches |

## 4. DEFINIZIONI

Per tutte le definizioni dei termini inerenti la privacy usati in tale documento si fa riferimento all'**art. 4** del **Regolamento UE 2016/679 "Regolamento Generale per la protezione dei dati"**. Laddove ritenuto necessario, nel corpo del documento saranno date le informazioni relative a termini e/o acronimi usati nel testo.

## 5. RESPONSABILITÀ

Le responsabilità sono descritte nel corpo del documento.

## 6. GESTIONE DEI DATA BREACH

### 6.1 GENERALITÀ

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

Per gestione del **Data Breach** (violazione dei dati) s'intende il coordinamento complessivo della risposta organizzativa ad una possibile crisi in modo efficace e tempestivo, con lo scopo di evitare o minimizzare i danni alla reputazione ed alla capacità di operare dell'**Istituzione Scolastica**.

In caso di **incidente** devono essere considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'**Istituzione Scolastica**.

Garantita l'incolumità fisica delle persone, le situazioni di crisi, in particolare quelle che riguardano sistemi informatici ma non solo, devono immediatamente essere comunicate all'**Amministratore del sistema** e al **Responsabile della Protezione dei Dati** (**RPD**) che provvederanno, in linea generale, a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema;
4. ripristinare il sistema;
5. effettuare test di operatività;
6. ripristinare e far riprendere l'operatività normale;
7. documentare tutte le operazioni.

Inoltre occorre garantire tutto quanto previsto dagli artt. 33 e 34 del **GDPR** in termini di comunicazione al **Garante** e agli **interessati** degli effetti della violazione.

## 6.2 TIPOLOGIE DI DATA BREACH

**Violazione di dati personali (data breach)** – È una violazione di sicurezza che comporta accidentalmente o in modo illecito:

- **la distruzione, e/o**
- **la perdita, e/o**
- **la modifica, e/o**
- **la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati.**

**S'intende per:**

- **Distruzione dei dati**
  - Non esistono più i dati;
  - Non esistono più in forma che possa essere utilizzata dal Titolare.
- **Perdita dei dati**
  - Il Titolare non ha più il controllo dei dati;
  - Il Titolare non ha più i dati.
- **Modifica dei dati**
  - Alterazione del dato;
  - Corruzione del dato;
  - Incompletezza del dato.
- **La divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati**
  - Divulgazione dei dati;

- Accesso ai dati da parte di destinatari non autorizzati;
- Trattamenti in violazione del **GDPR**.

## 6.3 ATTIVITÀ DI SEGNALAZIONE, RACCOLTA INFORMAZIONI, VALUTAZIONE, NOTIFICA DELLA VIOLAZIONE

| STEP | ATTIVITÀ | CHI | A CHI | QUANDO | COME |
|---|---|---|---|---|---|
| 1 | **Rilevazione e segnalazione di data breach** | Tutto il personale, collaboratori, Responsabili esterni | Amministratore di Sistema (AS) – Titolare – RPD | Appena se ne viene a conoscenza | Utilizzando le vie più brevi (telefono, di persona, e-mail) |
| 2 | **Raccolta informazioni sulla violazione** | L'**AS** o qualsiasi altra persona che per prima rileva la violazione o ne è informata o, comunque, è implicato nella situazione. Il Titolare deve dare precise istruzioni alla persona che lo ha contattato per iniziare subito la raccolta delle informazioni e/o dei documenti reputati necessari. | | Nel più breve tempo possibile | Con qualsiasi mezzo disponibile |
| 3 | **Comunicazione del data breach e registrazione delle informazioni** | L' **AS** o qualsiasi persona coinvolta che ha raccolto le informazioni. La registrazione sul modulo previsto può essere fatto da tale persona o dal Titolare con l'eventuale ausilio del RPD. | (Titolare); RPD, Esperti ICT | Appena ottenute le informazioni di base sulla violazione | Mod. 01P/P04 "Raccolta delle informazioni" |
| 4 | **Valutazione d'impatto** | Titolare che può richiedere l'ausilio di RPD, Esperti ICT, soggetti coinvolti | | Appena sono pronte tutte le informazioni | Mod. 03P/P04 "Autovalutazione" |
| 5 | **Individuazione delle azioni correttive e registrazione dell'evento** | Titolare che può richiedere l'ausilio di RPD, Esperti ICT, soggetti coinvolti | | Appena terminata la valutazione d'impatto | Analizzando i risultati della valutazione d'impatto. In questa fase si può incominciare ad effettuare la registrazione dell'evento sul mod. **02P/P04** |

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| | | | | | |
|---|---|---|---|---|---|
| | | | | | **"Registro data breach"** da parte del RPD |
| 6 | **Notifica della violazione (se necessaria, sulla base della valutazione d'impatto)** | Titolare/RPD | Garante | Entro 72 ore dalla rilevazione | Secondo la procedura on line predisposta sul sito del Garante |
| 7 | **Comunicazione agli interessati della violazione (se necessaria, sulla base della valutazione d'impatto)** | Titolare/RPD | Persone fisiche cui dati sono stati violati | Nei termini indicati nella valutazione d'impatto | Comunicazione diretta alle singole persone o mediante pubblicazione del sito loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate |
| 8 | **Disposizioni per l'attuazione delle misure correttive (se individuate)** | Responsabili delle Funzioni coinvolte | Soggetti incaricati di svolgere l'attività | Nei termini indicati nella valutazione d'impatto | Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione, le modalità di verifica di efficacia dell'azione correttiva |
| 9 | **Recepimento della risposta del Garante alla notifica (se effettuata)** | Titolare/RPD, Amministratore di Sistema, Responsabili delle Funzioni coinvolte, Esperti ICT | | | Disposizioni per l'attuazione delle eventuali azioni correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte |
| 10 | **Attuazione delle misure correttive e ripristino del sistema** | Amministratore di Sistema, Responsabili delle Funzioni coinvolte, Esperti ICT | | Nei termini indicati nella valutazione d'impatto e, comunque, il prima possibile | Secondo quanto indicato nelle attività da attuare |



| | | | | | |
|---|---|---|---|---|---|
| 11 | **Controllo dell'attuazione delle attività e verifica di efficacia delle azioni correttive** | RPD/ Amministratore di Sistema, Responsabili Funzioni coinvolte, Esperti ICT | | Nei termini indicati nella valutazione d'impatto e, comunque, il prima possibile | Secondo quanto indicato nelle attività da attuare |

## 6.4 ATTIVITÀ RELATIVE ALLE REGISTRAZIONE DELL'INCIDENTE

| STEP | ATTIVITÀ | CHI | A CHI | QUANDO | COME |
|---|---|---|---|---|---|
| 1 | **Registrazione della violazione/ aggiornamenti** | RPD | | Appena ricevuta la comunicazione | Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando successivi aggiornamenti |
| 2 | **Registrazione della risposta del Garante** | RPD | | Al momento della ricezione | Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in esse contenute |
| 3 | **Registrazione della prosecuzione/ chiusura dell'incidente** | RPD | | | Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per ulteriori indagini |

## 6.5 ATTIVITÀ INERENTI LA PROSECUZIONE DELLE INDAGINI

| STEP | ATTIVITÀ | CHI | A CHI | QUANDO | COME |
|---|---|---|---|---|---|
| 1 | **Prosecuzioni delle indagini** | Titolare/RPD, Amministratore di Sistema, Responsabili delle Funzioni coinvolte, Esperti ICT | | A seguito di indicazioni da parte del Garante o del Titolare se previsto nella prima valutazione d'impatto se le informazioni raccolte risultino incomplete o mancanti | Raccogliendo le informazioni mancanti o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine |
| 2 | **Esecuzione di nuova** | Titolare, RPD,Esperti ICT, soggetti coinvolti | | Al momento in cui si ritiene di aver raccolte | Utilizzando la metodologia definita |



| | | | | | |
|---|---|---|---|---|---|
| | **valutazione di impatto** | | | tutte informazioni necessarie | |
| 3 | **Comunicazione delle valutazioni del proseguimento delle indagini** | RPD | Titolare | Appena terminato il lavoro | Tramite breve relazione anche orale |
| 4 | **Aggiornamento della notifica della violazione (se necessaria sulla base della valutazione d'impatto)** | Titolare/RPD | Garante | Appena disponibili i dati o nei termini stabiliti dal Garante | Mediante modulistica predisposta dal garante |
| 5 | **Comunicazione agli interessati della violazione (se necessaria sulla base della valutazione della severità della violazione dei dati)** | Titolare/RPD | Persone fisiche cui dati sono stati violati | Nei termini indicati nella valutazione d'impatto | Comunicazione diretta alle singole persone o mediante pubblicazione del sito loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate |

## 6.6 LA NOTIFICA AL GARANTE

Al **Garante** vanno notificate unicamente le **violazioni di dati personali** che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali (**art. 33 par. 1** del **GDPR**).

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

La notifica deve contenere le informazioni previste all'**art. 33, par. 3** del **GDPR** e indicate nel **Provvedimento del Garante del 30 luglio 2019**, referenziato.

Per la notifica si utilizza il modello allegato al provvedimento di cui sopra e riportato nella documentazione di questa procedura.

Il **Titolare del Trattamento**, **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al **Garante** per la protezione dei dati personali.

Il **Responsabile del Trattamento** che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il **Titolare** in modo che possa attivarsi.

**Le notifiche al Garante effettuate oltre il termine delle 72 ore** devono essere **accompagnate dai motivi del ritardo.**

Il **Titolare del Trattamento**, a prescindere dalla **notifica** al **Garante**, **documenta** tutte le violazioni dei dati personali, utilizzando l'apposito registro, come descritto nei paragrafi precedenti. Tale documentazione consente all'**Autorità** di effettuare eventuali verifiche sul rispetto della normativa.

La **notifica** deve essere effettuata secondo le modalità riportate sul sito del **Garante** nell'apposita sezione dedicata al **data breach** seguendo in modo dettagliato e preciso quanto lì previsto.

## 6.7 LA NOTIFICA AGLI INTERESSATI

Se la violazione comporta un rischio elevato per i diritti delle persone, il **Titolare** deve comunicarla anche a tutti gli interessati (**art. 34 par. 1** del **GDPR**), utilizzando i canali più idonei, a meno che non abbia già preso misure tali da ridurne l'impatto, come descrito al **par. 6.5** (**punto 5** della tabella). La notifica va effettuata utilizzando un linguaggio chiaro e semplice e deve contenere almeno le informazioni previste dall'**art. 34 par. 2** del **GDPR** e cioè:

1. La natura della violazione dei dati personali;
2. Il nome e i dati di contatto del **Responsabile della Protezione dei Dati** (**DPO/RPD**) o di altro punto di contatto presso cui ottenere più informazioni;
3. Le probabili conseguenze della violazione dei dati personali;
4. Le misure adottate o di cui si propone l'adozione da parte del **Titolare del Trattamento** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

I canali da utilizzare per effettuare la comunicazione possono essere diversi a seconda della numerosità dei soggetti interessati da raggiungere e tra questi si possono identificare i seguenti:

a. Invio della comunicazione in formato **pdf** tramite **e-mail** o **pec** (se i soggetti interessati non sono molto numerosi);
b. Pubblicazione sul **sito web** in **area riservata** (se i soggetti interessati sono numerosi e di una categoria specifica, ad esempio docenti o dipendenti dell'**Istituzione Scolastica**) o in **area pubblica** (se i soggetti interessati sono numerosi e di varie categorie) con banner specifico presente in home page

## 6.8 VALUTAZIONE DELLA SEVERITÀ DELLA VIOLAZIONE DEI DATI

Qualunque sia il tipo di **data breach** esso va sempre registrato dal **Titolare del Trattamento** nel **Registro Trattamento Dati** dell'**Istituzione Scolastica** nella sezione specifica. Viceversa, per stabilire se è necessario effettuare la **comunicazione** al **Garante della protezione dei dati** e/o anche agli **interessati**, il **Titolare del Trattamento** (eventualmente con l'ausilo del **Responsabile della Protezione dei Dati**, **DPO/RPD**) deve effettuare una **valutazione d'impatto** della **violazione dei dati** così come riportato nei **flussi operativi** illustrati ai **par. 6.3** (**punto 4** del flusso operativo) e **6.5** (**punto 2** del flusso operativo) di questo documento. A tale scopo si fa riferimento alla **metodologia** riportata nel **Rif. [4]** presente nella tabella al **cap. 3** e che consente di valutare il parametro definito **severità del data breach**. Tale **metodologia** è stata sviluppata dalle **Autorità della Protezione dei Dati** (cd **Garante della Protezione dei dati**) di **Grecia** e **Germania** in collaborazione con l'**ENISA** (**European Union Agency for Network and Information Security** ossia l'**Agenzia dell'Unione Europea per la Sicurezza dell'Informazione e la Rete**).

Di seguito viene riportato solo il **metodo di calcolo** mentre si rimanda alla lettura del documento referenziato per ottenere i dettagli.

Definiamo i seguenti **parametri**:

| Simbolo | Definizione | Descrizione |
|---|---|---|
| **SE** | Severità della violazione dei dati | Stima dell'entità dell'impatto potenziale sugli individui derivante dalla violazione dei dati |
| **DPC** | Data Processing Context – Contesto del Trattamento Dati | Affronta il tipo di dati violati, insieme a una serie di fattori legati al contesto generale del trattamento |
| **EI** | Ease of Identification – Facilità d'Identificazione | Determina quanto facilmente l'identità degli individui può essere dedotta dai dati coinvolti nella violazione |

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| | | |
|---|---|---|
| **CB** | Circumstances of Breach – Circostanze della violazione | Affronta le circostanze specifiche della violazione, che sono legati al tipo di violazione, tra cui principalmente la perdita di sicurezza dei dati violati, nonché qualsiasi intento dannoso coinvolto |

Il valore della **Severità della violazione SE** sarà dato da:

**SE = (DPC x EI) + CB** (1)

In base ai valori assunti da **SE** si determina la **gravità della violazione** e la necessità o meno delle **segnalazioni** al **Garante** e/o agli **interessati**. Si fa riferimento alla seguente valorizzazione:

| **SEVERITÀ DELLA VIOLAZIONE DEI DATI** | | |
|---|---|---|
| **Valore** | **Grado** | **Descrizione** |
| **SE** < 2 | Basso | Gli individui non saranno interessati o possono incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo le informazioni, fastidi, irritazioni, ecc.). Non si ritiene necessaria alcuna notifica. |
| 2 ≤ **SE** < 3 | Medio | Gli individui possono incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, diniego di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.). **Effettuare la notifica al Garante; non si ritiene necessaria la notifica agli interessati**. |
| 3 ≤ **SE** < 4 | Alto | Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.). **Effettuare la notifica al Garante e agli interessati**. |
| **SE** ≥4 | Molto alto | Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come un debito sostanziale o incapacità di lavoro, disturbi psicologici o fisici a lungo termine, morte, ecc.). **Effettuare la notifica al Garante e agli interessati**. |

Al valore calcolato di **SE** si affiancano altri **indicatori** che, pur non modificando il valore ottenuto, risultano importanti per la valutazione complessiva. Tali **indicatori** sono:

1. **Il numero di individui violati supera 100**. I dati di un individuo, violati nel contesto di un incidente più grande, possono potenzialmente essere divulgati più facilmente, mentre allo stesso tempo un elevato numero di individui interessati influenza la scala complessiva della violazione.
2. **Dati Incomprensibili.** L'incomprensibilità (ad es. sotto forma di crittografia forte e senza compromessi di chiave) può ridurre notevolmente l'impatto per gli individui, in quanto riduce notevolmente la possibilità di parti non autorizzate che accedono ai dati.

Per effettuare il calcolo del valore di **SE** sulla base della **(1)** si può fare riferimento alle **valorizzazioni** dei **parametri** definiti sopra riportati nelle **tabelle** di seguito illustrate.

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| **Tabella 1 – Data Processing Context/ Contesto del Trattamento Dati (DPC)[1, 2]** | | **Valore** |
|---|---|---|
| **Dati semplici** | **Ad esempio, dati biografici, dettagli dei contatti, nome completo, dati sull'educazione, vita di famiglia, esperienza professionale, ecc.** | |
| | **Punteggio di base preliminare**: quando la violazione coinvolge "**dati semplici**" e il **Titolare** non è a conoscenza di eventuali fattori aggravanti. | **1** |
| | Il valore di **DPC** potrebbe essere aumentato di **1**, ad es. quando il volume dei **dati semplici** e/o le caratteristiche del **Titolare** sono tali da consentire una certa profilazione dell'individuo o si possono formulare ipotesi circa lo stato sociale/finanziario dell'individuo. | 2 |
| | Il valore di **DPC** potrebbe essere aumentato di **2**, ad es. quando i **dati semplici** e/o le caratteristiche del **Titolare** possono portare a supposizioni sullo stato di salute dell'individuo, le preferenze sessuali, le convinzioni politiche o religiose. | 3 |
| | Il valore di **DPC** potrebbe essere aumentato di **3**, ad es. quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), le informazioni possono essere fondamentali per la loro sicurezza personale o condizioni fisiche/psicologiche. | 4 |
| | | |
| **Dati Comportamentali** | **Ad es. localizzazione, dati di traffico, dati sulle preferenze e abitudini personali, ecc.** | |
| | **Punteggio di base preliminare**: quando la violazione coinvolge "**dati comportamentali**" e il **Titolare** non è a conoscenza di eventuali fattori aggravanti o riducenti. | **2** |
| | Il valore di **DPC** potrebbe essere ridotto di 1, ad es. quando la natura dell'insieme di dati non fornisce alcuna informazione sostanziale sulle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (ad es. combinazione di informazioni provenienti da ricerche web). | 1 |
| | Il valore di **DPC** può essere aumentato di 1, ad es. quando il volume dei dati comportamentali e/o le caratteristiche del **Titolare** sono tali che un profilo dell'individuo può essere creato, esponendo informazioni dettagliate sulla sua vita quotidiana e le sue abitudini. | 3 |
| | Il valore di **DPC** può essere aumentato di 2, ad es. se è possibile creare un profilo basato sui dati sensibili di un individuo. | 4 |
| | | |

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| **Tabella 1 – Data Processing Context/ Contesto del Trattamento Dati (DPC)[1, 2] (continua)** | | **Valore** |
|---|---|---|
| **Dati Finanziari** | **Qualsiasi tipo di dati finanziari (ad es. entrate, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito, fatture, ecc.). Comprende i dati relativi all'assistenza sociale relativi alle informazioni finanziarie.** | |
| | **Punteggio di base preliminare**: quando la violazione coinvolge "**dati finanziari**" e il **Titolare** non è a conoscenza di eventuali fattori aggravanti o riducenti. | **3** |
| | Il valore di **DPC** potrebbe essere ridotto di 2, ad es. quando la natura dell'insieme dei dati non fornisce alcuna informazione sostanziale sulle informazioni finanziarie della persona (ad es. il fatto che una persona è cliente di una certa banca senza ulteriori dettagli). | 1 |
| | Il valore di **DPC** potrebbe essere ridotto di 1, ad es. quando l'insieme dei dati specifico include alcune informazioni finanziarie, ma non fornisce ancora alcuna informazione significativa sullo stato/sulla situazione finanziaria dell'individuo (ad es. numeri di conto bancari semplici senza ulteriori dettagli). | 2 |
| | Il valore di **DPC** potrebbe essere aumentato di 1, ad es. quando a causa della natura e/o del volume del set di dati specifico, vengono divulgate informazioni finanziarie complete (ad es. carta di credito) che potrebbero consentire frodi o viene creato un profilo sociale/finanziario dettagliato. | 4 |
| | | |
| **Dati sensibili** | **Qualsiasi tipo di dati sensibili (ad es. salute, affiliazione politica, vita sessuale)** | |
| | **Punteggio di base preliminare**: quando la violazione coinvolge "**dati sensibili**" e il **Titolare** non è a conoscenza di eventuali fattori riducenti. | **4** |
| | Il valore di **DPC** potrebbe essere portato a 1, ad es. quando la natura dell'insieme dei dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (ad es. combinazione di informazioni provenienti da ricerche Web). | 1 |
| | Il valore di **DPC** potrebbe essere portato a 2, ad es. quando la natura dei dati può portare a ipotesi generali. | 2 |
| | Il valore di **DPC** potrebbe essere ridotto di 1, ad es. quando la natura dei dati può portare a ipotesi su informazioni sensibili. | 3 |

**Note:**

1. Se i **dati violati** sono di **diversa natura** (ad es., dati semplici e dati finanziari) con una **valorizzazione diversa**, nella **(1)** va inserito il **valore più alto** determinato;

2. Nell'effettuare la valorizzazione del fattore **DPC** occorre considerare alcuni fattori che possono portare o ad un incremento o a un decremento della valorizzazione:
   a. **Fattori aggravanti**:
      i. **Volume dei dati violati:** sia in termini di **tempo** (i dati possono riguardare periodi più o meno lunghi di tempo, 1 anno, 1 mese, ecc.) sia in termini di **contenuto** (a complemento di dati dello stesso tipo).
      ii. **Caratteristiche speciali degli interessati**: il valore di **DPC** di base di un determinato insieme di dati potrebbe anche essere aumentato nel caso in cui gli interessati appartengano a un gruppo sociale con esigenze particolari (ad esempio minori, individui di un determinato gruppo con caratteristiche speciali).
   b. **Fattori riducenti:**
      i. **Invalidità / inesattezza dei dati:** il valore di **DPC** di base di un determinato insieme di dati può essere ridotto se l'invalidità o inesattezza dei dati sono note al Titolare del Trattamento (ad esempio a causa della loro età o contenuto) e, quindi, il loro significato è ridotto. Il Titolare deve essere certo di questa circostanza per includerlo nella valutazione.
      ii. **Disponibilità pubblica:** il valore di **DPC** di base di un determinato insieme di dati può anche essere ridotto nel caso in cui i dati violati fossero già disponibili al pubblico prima della violazione o possano essere facilmente raccolti e / o consultati tramite fonti pubblicamente disponibili.
      iii. **Natura dei dati:** un altro fattore decrescente potrebbe in alcuni casi essere la natura stessa di un particolare insieme di dati che, nonostante il valore di **DPC** iniziale, ha un significato inferiore, in termini di informazioni che può rivelare sull'individuo. Questo è, ad esempio, il caso di un **certificato medico** che certifica che l'individuo è in buono stato di salute senza rivelare altre informazioni. In questo caso, anche se il punteggio di base sarebbe 4 a causa dei dati sanitari che sono dati sensibili, il punteggio **DPC** finale del set di dati specifico sarebbe 1, poiché non può di per sé influire sulla vita personale dell'individuo. Questo fattore, tuttavia, dovrebbe essere considerato con grande cura e chiara spiegazione del motivo per cui un particolare trattamento dei dati è per natura inferiore al suo valore di **DPC** di base.

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| **Tabella 2 – Ease of Identification/ Facilità d'Identificazione (EI)[3, 4]** | | **Valore** |
|---|---|---|
| **Nome completo (nome e cognome)** | È considerato come l'identificatore diretto più comune, ma il valore di **EI** può variare a seconda dei casi, poiché il nome completo non sempre di per sé individua in modo univoco l'individuo. Ad esempio, quando l'identificazione viene effettuata utilizzando solo il nome completo dell'individuo: | |
| | **(l'Effetto è Trascurabile)** se considerando l'intera popolazione di un paese in molti condividono lo stesso nome completo. | 0,25 |
| | **(l'Effetto è limitato)** se considerando l'intera popolazione di un paese poche persone condividono lo stesso nome completo. | 0,50 |
| | **(l'Effetto è significativo)** se considerando l'intera popolazione di una piccola città poche o nessuna persona condivide lo stesso nome completo. | 0,75 |
| | **(l'Effetto è massimo)** se considerando l'intera popolazione di un paese si utilizza anche la data di nascita e l'indirizzo e-mail | 1 |
| | | |
| **Codice Carta d'identità/ Codice Passaporto/ Codice fiscale** | Sono tutti considerati identificativi unici e possono essere utilizzati per individuare l'individuo, purché sia possibile collegarli a una banca dati di riferimento (ad es. collegando un numero di carta d'identità a una persona particolare). Ad esempio, quando l'identificazione viene eseguita utilizzando solo uno di questi numeri: | |
| | **(l'Effetto è Trascurabile)** quando non vengono fornite altre informazioni sull'individuo o non è possibile trovare informazioni aggiuntive, a meno che non si ottenga l'accesso alla banca dati di riferimento. | 0,25 |
| | **(l'Effetto è significativo)** quando l'identificatore rivela ulteriori informazioni identificative sull'individuo (ad es., numero di previdenza sociale indicante la data di nascita) ed è collegato ad altri dati (ad es. indirizzo postale o e-mail). | 0,75 |
| | **(l'Effetto è massimo)** quando sono disponibili anche informazioni dalla banca dati di riferimento (ad es. carta d'identità e nome completo e/o immagine). | 1 |
| | | |
| **Numero di telefono/ Indirizzo di residenza** | Sono entrambi identificatori indiretti, che possono essere utilizzati anche per comunicare o accedere all'individuo. Quando l'identificazione è basata solo su uno di questi due identificatori: | |
| | **(l'Effetto è Trascurabile)** se considerando l'intera popolazione di un paese il numero/indirizzo non è registrato in un registro accessibile al pubblico. | 0,25 |
| | **(l'Effetto è limitato)** se considerando l'intera popolazione di una piccola città il numero/indirizzo non è registrato in un registro accessibile al pubblico (identificazione possibile tramite comunicazione). | 0,50 |



| | | |
|---|---|---|
| | **(l'Effetto è massimo)** se considerando l'intera popolazione del paese il numero/indirizzo è incluso nel registro accessibile al pubblico. | 1 |

| **Tabella 2 – Ease of Identification/ Facilità d'Identificazione (EI)[3, 4] (continua)** | | **Valore** |
|---|---|---|
| **Indirizzo email** | È anch'esso un identificatore indiretto, che può essere utilizzato per comunicare con l'individuo e in alcuni casi può includere informazioni sul suo nome (nome e/ o cognome). Quando l'identificazione è basata su e-mail: | |
| | **(l'Effetto è Trascurabile)** quando l'indirizzo email non rivela altre informazioni identificative (ad es. nome) e non viene utilizzato come indirizzo primario dell'individuo nei siti internet, nei forum o nei social network. | 0,25 |
| | **(l'Effetto è significativo)** quando l'indirizzo di posta elettronica non rivela altre informazioni identificative (ad es. nome) ma viene utilizzato come indirizzo primario dell'individuo in siti internet, forum o social network (consultabile sul web). | 0,75 |
| | **(l'Effetto è massimo)** quando l'indirizzo e-mail rivela il nome dell'individuo e viene utilizzato come suo indirizzo principale in siti internet, forum o social network (ricercabili sul web). | 1 |
| | | |
| **Immagine (foto e/o video)** | Può essere un identificatore diretto o indiretto, a seconda dei casi. Ad esempio, quando l'identificazione è basata solo su un'immagine: | |
| | **(l'Effetto è Trascurabile)** quando l'immagine non è chiara o vaga (ad es. riprese CCTV ossia riprese televisive a circuito chiuso come quelle della videosorveglianza da una lunga distanza). | 0,25 |
| | **(l'Effetto è limitato)** quando l'immagine è poco chiara o vaga, ma include informazioni aggiuntive (ad es. ambiente che mostra una posizione specifica) che potrebbero portare all'identificazione dell'individuo. | 0,50 |
| | **(l'Effetto è significativo)** quando l'immagine è chiara ma non vi sono altre informazioni identificative ad essa collegate. | 0,75 |
| | **(l'Effetto è massimo)** quando l'immagine è chiara e collegata ad alcune informazioni aggiuntive (ad es. informazioni sull'appartenenza a un gruppo specifico, indirizzo di casa, ecc.). | 1 |
| | | |

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| | | |
|---|---|---|
| **Codifica/ Pseudonimi/ Iniziali** | La **codifica** si riferisce all'assegnazione di un numero ID univoco a ciascun individuo, ad es. nel contesto di un database specifico. L'uso di **pseudonimi** è una forma di **pseudonimizzazione**, nel senso che un identificatore specifico (di solito il nome completo dell'individuo) è sostituito da un **alias** (pseudonimo). Le **iniziali** sono un tipo di **alias** che viene estratto dal nome completo dell'individuo. Come nel caso degli identificatori univoci, i codici e gli alias possono essere utilizzati per identificare l'individuo finché è possibile collegarli a una banca dati di riferimento (ad es. collegando il codice/alias al nome completo di una persona particolare). Quando l'identificazione è basata sulla codifica o sull'uso di pseudonimi: | |
| | **(l'Effetto è Trascurabile)** quando il codice/pseudonimo non rivela e non può essere collegato a nessun altro dato personale relativo all'individuo a meno che non si ottenga l'accesso al database di riferimento. | 0,25 |
| | **(l'Effetto è significativo)** quando lo pseudonimo rivela alcuni dati sull'individuo (ad es. nome) ed è collegato ad altri dati personali (ad es. indirizzo e-mail dell'individuo). | 0,75 |
| | **(l'Effetto è massimo)** quando lo pseudonimo rivela il nome completo dell'individuo o sono disponibili anche i dati del database di riferimento. | 1 |

**Nota:**

3. Se i **dati violati** sono di **diversa natura** (ad es., indirizzo email e numeri di telefono) con una **valorizzazione diversa**, nella **(1)** va inserito il **valore più alto** determinato;
4. L'identificazione può essere diretta o indiretta ed è effettuata con l'utilizzo di determinati identificatori, tenendo conto anche del contesto generale del trattamento dei dati personali. Gli esempi riportati nella tabella mostrano un elenco (non esaustivo) di identificatori comuni e diversi casi del loro possibile uso per determinare il valore di **EI**. Va notato che in molti casi la violazione comprenderà una combinazione di diversi identificatori, che aumenta automaticamente la facilità di identificazione. Questo è un elemento molto importante che dovrebbe essere preso in considerazione dal **Titolare del Trattamento** e si riflette negli esempi riportati nella tabella.

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

| **Tabella 3 – Circumstances of Breach – Circostanze della violazione (CB)[5]** | | **Valore** |
|---|---|---|
| **Perdita di riservatezza** | La **perdita di riservatezza** si ha quando **i dati sono a disposizione di terzi non autorizzati**. | |
| | Dati esposti a **rischi di riservatezza senza prove di trattamento illecito**. Ad esempio:<br>• Un file cartaceo o un laptop vengono persi durante il trasferimento.<br>• Le attrezzature sono state smaltite senza distruzione dei dati personali. | 0 |
| | Dati esposti a **rischi di riservatezza perché forniti a destinatari noti**. Ad esempio:<br>• Una e-mail con dati personali è stata erroneamente inviata a un certo numero di destinatari noti.<br>• Alcuni clienti potrebbero accedere ai conti di altri clienti in un servizio online. | + 0,25 |
| | Dati esposti a **rischi di riservatezza perché ceduti a un numero sconosciuto di destinatari**. Ad esempio:<br>• I dati sono pubblicati su una bacheca internet.<br>• I dati vengono caricati su un sito P2P (ossia Peer-to-Peer).<br>• Un dipendente vende un CD ROM con i dati dei clienti.<br>• Un sito Web erroneamente configurato rende pubblicamente accessibili i dati su Internet dagli utenti interni. | + 0,50 |
| | | |
| **Perdita d'integrità** | La **perdita di integrità** si ha quando **i dati sono stati alterati (modificati) in modo illecito o incosapevole** | |
| | Dati esposti a **rischi d'integrità** perché modificati ma senza alcun **utilizzo errato o illecito identificato**. Ad esempio:<br>• Le registrazioni di una banca dati con dati personali sono state erroneamente aggiornate, ma l'originale è stato ottenuto prima che qualsiasi utilizzo dei dati modificati si sia verificato. | 0 |
| | Dati esposti a **rischi d'integrità** perché alterati ed eventualmente **utilizzati in modo scorretto o illegale ma con possibilità di recupero**. Ad esempio:<br>• Un record che è necessario per la fornitura di un servizio sociale online è stato modificato e l'interessato ha bisogno di chiedere il servizio in modo offline.<br>• Un record che è importante per l'accuratezza del fascicolo di un interessato in un servizio medico online è stato cambiato. | 0,25 |



| | | |
|---|---|---|
| | Dati esposti a **rischi d'integrità** perché alterati ed eventualmente **utilizzati in modo scorretto o illegale senza possibilità di recupero**. Ad esempio:<br>• Gli stessi esempi del punto precedente, solo che non è possibile recuperare l'originale. | 0,50 |

| **Tabella 3 – Circumstances of Breach – Circostanze della violazione (CB)[4] (continua)** | | **Valore** |
|---|---|---|
| **Perdita di disponibilità** | La **perdità di disponibilità** si ha quando i dati **non sono più presenti** presso il **Titolare** (furto, distruzione, cancellazione, ecc.) | |
| | I dati sono stati **persi** ma è possibile **ripristinarli senza alcuna difficoltà**. Ad esempio:<br>• Una copia di un fascicolo o di un documento è andata persa ma sono disponibili altre copie.<br>• Un database è danneggiato ma può essere facilmente ricostruito da altri database. | 0 |
| | I dati sono stati **persi** ma l'indisponibilità è temporanea. Ad esempio:<br>• Un database è danneggiato ma può essere ricostruito da altri database, anche se è necessaria qualche elaborazione.<br>• Un file viene perso ma le informazioni possono essere fornite nuovamente dall'interessato. | 0,25 |
| | I dati sono stati **persi** e l'indisponibilità è **totale** (i dati non possono essere recuperati in alcun modo dal Titolare o dall'interessato). Ad esempio:<br>• Un file è perso/ database danneggiato, non c'è il backup di queste informazioni, e non può essere fornito dall'interessato | 0,50 |
| | | |
| **Intento doloso** | La **violazione** può essere dovuta ad un **errore**, umano o tecnico (ad esempio perdita accidentale, smaltimento inadeguato, errore umano e bug software o errore di configurazione), oppure da un'**azione intenzionale** con lo scopo di danneggiare il **Titolare del Trattamento** e/o l'**interessato** o per conseguire un interesse personale illecito (ad esempio, furto, azione di hackeraggio per ransomware o altro intento illecito e/o scopo di lucro personale). | |
| | La **violazione** non è riconducibile ad un **atto doloso** inteso a danneggiare il **Titolare** e/o l'**interessato** o per qualsiasi altro scopo illecito. | 0 |
| | La **violazione** è dovuta ad un'**azione intenzionale**, ad es. per causare problemi al **Titolare del Trattamento** (ad es. dimostrare la perdita di sicurezza) e/o per danneggiare le persone. Ad esempio:<br>• Un dipendente di una società condivide intenzionalmente i dati privati dei clienti in un sito pubblico di social media.<br>• Un dipendente di un'azienda vende dati privati dei clienti a un'altra azienda. | 0,50 |

| | | |
|---|---|---|
| | • Un membro di un social network invia intenzionalmente informazioni su altri membri ai loro familiari al fine di danneggiarli. | |

**Nota:**

5. Poiché in una **singola violazione** possono intervenire diversi tipi di **Circostanze della violazione** (ad esempio, si ha una **perdita di disponibilità** per un **intento doloso**), nella **(1)** va inserito il **valore** che si ottiene **sommando i valori** determinati per ogni singola circostanza riscontrata.

*ISTITUTO COMPRENSIVO STATALE*

*"Antonio De Curtis" - Casavatore (NA)*

## 7. MODULI E ALLEGATI

| | |
|---|---|
| **Mod. 01P/P04** | Raccolta delle informazioni |
| **Mod. 02P/P04** | Registro Data Breach |
| **Mod. 03P/P04** | Autovalutazione data breach |