

I.I.S. "GOBETTI MARCHESINI CASALE ARDUINO" - -TORINO
Prot. 0013279 del 14/09/2026
I-4 (Uscita)

Modello di gestione del Data Breach

Riferimento normativo:

**-REGOLAMENTO UE N. 679/2016
(GDPR)**

Linee guida del Garante per la Protezione dei dati personali

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013



1. PREMESSE

Il presente documento ha lo scopo di descrivere le modalità operative da seguire per la rilevazione di eventuali violazioni di dati personali (c.d. "*data breach*"), la loro segnalazione, la valutazione e l'eventuale notifica all'Autorità Garante per la protezione dei dati personali e se necessario agli interessati, nel rispetto di quanto previsto dagli artt. 33 e 34 del Regolamento (UE) n. 2016/679 General Data Protection Regulation (di seguito solo GDPR), nonché delle Linee guida del Garante per la protezione dei dati personali e del Comitato Europeo per la protezione dei dati (European data protection board).

2. PRINCIPALI DEFINIZIONI

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1 GDPR).

Dati particolari: dati personali che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale e il trattamento di dati genetici, dati biometrici, dati riguardanti la salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica (art. 9, co.1 GDPR).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2 GDPR).

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali (art. 4, punto 7 GDPR). Nel prosieguo inteso come Istituto Gobetti marchesini Casale Arduino

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, punto 8 GDPR).

Interessato: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

Data Protection Officer (DPO): la persona nominata come responsabile della protezione dei dati ai sensi dell'art. 37 del GDPR.

Violazione di dati personali (data breach): la violazione 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, punto 12 GDPR).

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013



- PROCEDURA DI GESTIONE DEL DATA BREACH

o Rilevazione dell'incidente di sicurezza

Qualsiasi dipendente (previamente autorizzato al trattamento dei dati personali) o responsabile del trattamento che viene a conoscenza di un incidente di sicurezza, di una potenziale violazione di dati personali o che riceva una segnalazione a tale riguardo, deve informare immediatamente il Titolare del trattamento, il DPO e il referente privacy (se presente).

o Analisi preliminare

Il Titolare del Trattamento, con il supporto del referente privacy ed il coinvolgimento del DPO, analizzano l'accaduto al fine di valutare se la violazione di dati personali si sia effettivamente verificata, considerando:

- natura della potenziale violazione di dati personali;
- processi aziendali e sistemi informatici interessati;
- categorie e numero approssimativo di dati interessati;
- categorie e numero approssimativo dei soggetti interessati;
- possibili/probabili conseguenze della violazione dei dati personali, sia per l'organizzazione del Titolare che per gli interessati, compresi potenziali danni economici e alla reputazione;
- misure tecniche/organizzative (con particolare riferimento all'indicazione delle misure non adottate o, se adottate, a quelle aggirate).

Se all'esito dell'analisi emerge la conferma che si tratta di una violazione di dati personali, il Titolare del trattamento, è tenuto ad adottare tempestivamente tutte le misure necessarie per porre rimedio agli effetti avversi di tale violazione.

o Valutazione dei rischi per i diritti e le libertà degli interessati

Per comprendere la severità o meno di una violazione dei dati personali è necessario valutare le conseguenze che derivano da essa, considerando in particolare l'impatto che la violazione dei dati personali può avere per i diritti e le libertà degli interessati. La valutazione deve includere un'adeguata considerazione delle circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che ciò si verifichi.

Per valutare il livello di rischio associato ad una violazione dei dati personali, anzitutto bisogna contestualizzare la violazione. I dati personali devono essere classificati in categorie, che a titolo esemplificativo possono essere le seguenti:

- dati comuni (es. dati anagrafici, dati di contatto, esperienze professionali, etc.);
- dati particolari (es. informazioni che rivelano l'origine razziale o etnica, opinioni politiche, credenze religiose, dati relativi alla salute).
- dati finanziari (dei dipendenti, di terzi).

Dopo aver individuato le categorie di dati oggetto della violazione, bisogna considerare altre circostanze, quali:

- il volume dei dati (es. dati che riguardano l'Ente in generale o un singolo settore)
- le caratteristiche dei soggetti (es. se oggetto di violazione sono dati che riguardano i minori, la tutela dovrà essere rafforzata);
- la pubblicità del dato (es. se il dato è a vario titolo già pubblico)
- inutilizzabilità dei dati (es. se i dati non sono resi inaccessibili o indisponibili all'utilizzo,).

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

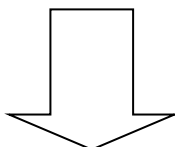
Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013

Al fine di individuare le azioni da intraprendere a seguito di una violazione dei dati personali, il Garante consiglia di procedere attraverso tecniche di autovalutazione, utilizzando le linee guida predisposte a tale scopo, come indicate nel seguente documento (Allegato A).



Allegato A

**QUESTIONARIO DI AUTOVALUTAZIONE (SELF-ASSESSMENT) PER
INDIVIDUARE LE AZIONI DA INTRAPRENDERE A SEGUITO DI UNA
VIOLAZIONE DEI DATI PERSONALI**

-Linee guida Garante per la protezione dei dati personali – www.garanteprivacy.it

1) Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità dei dati?

☐ sì ☐ no

N.B. Un incidente di sicurezza è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti da un'organizzazione, mettendo a rischio uno dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità.

Esempi: Un incidente di sicurezza può verificarsi in seguito ad un attacco informatico, ad un comportamento umano illecito o accidentale, ad una catastrofe naturale, ad un malfunzionamento di hardware o software.

Se la risposta è sì, la domanda successiva è:

2) L'incidente di sicurezza ha coinvolto dati personali? (Per la definizione delle categorie di dati personali, si veda la pagina 2. del presente documento).

☐ sì ☐ no

Se la risposta è sì, si è verificato un violazione di dati (data breach).

La violazione di dati può consistere ad esempio:

-nell'accesso ai dati personali da parte di terzi non autorizzati;

-nella perdita di riservatezza a seguito dell'invio di una mail o di una pec contenente dati personali ad un destinatario errato;

-nella perdita o furto di un dispositivo o di un supporto di memorizzazione contenente dati personali (es. pen-drive, unità esterne, ecc.);

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013



-nella perdita di disponibilità dei dati archiviati in un database, attraverso un ransomware o altro tipo di malware;

-nella perdita di disponibilità dei dati personali se, ad esempio, tali dati sono stati accidentalmente cancellati in maniera definitiva o resi temporaneamente indisponibili a causa dell'interruzione di un servizio.

3)E' probabile che la violazione presenti un rischio per i diritti e le libertà degli interessati?

☐ sì ☐ no

Il rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale, per le persone fisiche i cui dati sono stati violati.

Il considerando 85 del GDPR, elenca alcuni danni che possono derivare da una violazione di dati personali, quali ad esempio: la discriminazione, il furto o l'usurpazione di identità, perdite finanziarie, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale, la decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo.

In caso di violazione di dati personali *"Il titolare del trattamento notifica la violazione all'autorità di controllo, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche"* (art. 33, par. 1 GDPR e art. 26 D.lgs 51/2018).

Il Garante precisa, quindi, che se è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche – cioè è improbabile che dalla violazione possa derivare un impatto negativo per le persone fisiche e il titolare sia in grado di dimostrarlo – la violazione occorsa non è soggetta all'obbligo di notifica all'Autorità di controllo.

Al fine di valutare adeguatamente il potenziale rischio per le persone fisiche, bisogna considerare diversi fattori, tra cui: tipo di violazione; natura, carattere sensibile e volume dei dati personali; facilità di identificazione delle persone fisiche; gravità delle conseguenze per le persone fisiche; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento; numero di persone fisiche interessate;

Esempi di violazioni che potrebbero non presentare rischi per gli interessati, e quindi non essere soggette all'obbligo di notifica all'Autorità di controllo sono:

- la violazione di dati personali già disponibili pubblicamente, in quanto potrebbe risultare improbabile il verificarsi di un danno fisico per gli interessati conseguente alla divulgazione di dati già pubblici;
- la perdita o il furto di una pen-drive contenente dati personali crittografati, di cui è disponibile un backup che consente un'integrale e tempestivo ripristino dei dati.

4)La violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche?

☐ sì ☐ no

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013



"Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo" (art. 34, par. 1 GDPR e art. 27 D.Lgs 51/2018).

ADEMPIMENTI DEL TITOLARE A SEGUITO DI UN DATA BREACH: LA NOTIFICA AL GARANTE PRIVACY E LA COMUNICAZIONE AI SOGGETTI INTERESSATI

All'esito della procedura di autovalutazione, qualora sia stata accertata la violazione, stabilita la natura e l'intensità della stessa nonché gli interessati colpiti dall'incidente di sicurezza, il Titolare, coadiuvato dal DPO e dal Referente privacy, dovrà provvedere alla relativa notifica al Garante e se necessario alla comunicazione agli interessati.

"In caso di violazioni di dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente, a norma dell'art. 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 dai motivi del ritardo". (art. 33, par. 1 GDPR, e art. 26 D.Lgs 51/2018).

Il Garante chiarisce che il titolare può considerarsi *"a conoscenza della violazione"* nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha comportato la compromissione di dati personali.

4.1 Contenuto della notifica al Garante

La notifica deve contenere le informazioni previste dall'art. 33, par. 3 del GDPR e precisamente:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle 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 attenuare i possibili effetti negativi.

N.B. *"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive, senza ulteriore ingiustificato ritardo" (art. 33, par. 4 GDPR)*

In tal caso il titolare, al momento della notifica, deve indicare se si tratta di una notifica preliminare, impegnandosi a comunicare tutte le informazioni e i dettagli circa la violazione occorsa non appena disponibili e senza ingiustificato ritardo, attraverso una notifica integrativa.

4.2 Come inviare la notifica La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo: protocollo@pec.gpdp.it, oppure tramite posta elettronica ordinaria all'indirizzo:

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013



protocollo@gpdp.it e deve essere sottoscritta digitalmente ovvero con firma autografa. In quest'ultimo caso, la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

N.B. Per procedere alla notifica al Garante, il Titolare – IS Gobetti Marchesini Casale Arduino utilizza il modello ufficiale di notifica, emesso dal Garante in data 30 Luglio 2019, disponibile nell'area privacy al sito

4.3 Comunicazione della violazione agli interessati

Oltre alla notifica al Garante, ***“Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo”***. (art. 34 par. 1 del GDPR e art. 27 del D.Lgs 51/2018).

L'obiettivo della comunicazione consiste nel fornire agli interessati stessi informazioni specifiche sulle misure che questi possono adottare per proteggersi.

La comunicazione agli interessati coinvolti deve fornire ***“con linguaggio semplice e chiaro”*** (art. 34, par. 2 GDPR e art. 27 D.Lgs 58/2018):

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle 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 attenuare i possibili effetti negativi.

La violazione sarà comunicata dal Titolare agli interessati coinvolti (ad es. mediante messaggio di posta elettronica o comunicazione postale), a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procederà a una comunicazione pubblica o a una misura simile (ad esempio banner o notifiche su siti web di primo piano, pubblicità di rilievo sulla stampa) che permetta di informare gli interessati con analoga efficacia (art. 34, par. 3 lett. c) GDPR).

4.4 La tenuta del registro delle violazioni

“Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo”. (art. 33, par. 5 GDPR).

Il Garante chiarisce che il titolare del trattamento, a prescindere dalla notifica al Garante (e dunque anche in quei casi in cui nelle suindicate ipotesi questa non dovesse risultare necessaria), documenta tutte le violazioni di dati personali, ad esempio predisponendo un apposito registro.

A tal fine **IS Gobetti Marchesini Casale Arduino**, utilizza il “registro delle violazioni di dati”, presente in area privacy del sito istituzionale

Il Dirigente Scolastico
Prof.ssa Maria De Pietro

MARIA DE PIETRO
14.09.2026 15:44:39
CEST

Sede legale

GOBETTI MARCHESINI CASALE ARDUINO
Corsi diurni e serali
Via Figlie dei Militari, 25 10131 Torino Tel. 011.0898342
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.176/00

Sede associata

CASALE - corsi diurni
Via Rovigo, 19 10152 Torino Tel. 011.0898477
Certificazione di Qualità UNI EN ISO 9001 - 2015 Certificato n°620
Accreditamento della Regione Piemonte per la Formazione certificato n.163/001

Sede associata

Sezione Ospedaliera OIRM
Piazza Polonia, 94 10126 Torino Tel. 011.3135013

