

ISTRUZIONI OPERATIVE GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

1. ABBREVIAZIONI

CCO:	Coordinatore <i>Clinical Operations</i>
DO:	<i>Direttore Operativo</i>
DM:	<i>Data Manager</i>
DPO:	<i>Data Protection Officer</i>
FROM – E.T.S.:	FROM-Fondazione per la Ricerca Ospedale di Bergamo – Ente del Terzo Settore
GCP:	<i>Good Clinical Practice</i>
GDPR:	<i>General Data Protection Regulation</i>
ICH:	<i>International Council of Harmonization</i>
ISF:	<i>Investigator's Site File</i>
MUA:	<i>Motore Unico Amministrativo</i>
PM:	<i>Project Manager</i>
POS:	<i>Procedura Operativa Standard</i>
TMF:	<i>Trial Master File</i>
UE:	Unione Europea

2. Scopo

La presente istruzione operativa ha lo scopo di descrivere il necessario flusso di attività da porre in essere nel momento in cui si sviluppi una violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento 679/2016/UE.

DATA EFFETTIVA 15/09/2023

1/6

Per data breach, in italiano “violazione dei dati personali”, si intende una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

Il Regolamento Europeo prevede che, in caso di violazione dei dati personali, il Titolare del trattamento debba notificare la violazione all’Autorità di controllo competente 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.

La gestione delle violazioni di dati personali avviene tramite il flusso “data breach” presente in MUA–Motore Unico Amministrativo con la compilazione di un questionario on-line e coinvolgerà le diverse unità organizzative che segnaleranno l’avvenuta violazione, la funzione interna competente in materia di protezione dei dati ed il Data Protection Officer (DPO).

Al MUA-Motore Unico Amministrativo hanno accesso il Direttore Operativo, il Referente Privacy e l’addetto alle registrazioni sul MUA.

3. *Casi nei quali avviare la procedura di gestione della violazione dei dati personali (data breach)*

I casi in cui sarà necessario applicare la presente istruzione sono, a titolo esemplificativo e non esaustivo:

- Sottrazione di credenziali di autenticazione
- Furto di PC, Notebook, Tablet, Smartphone contenenti dati personali
- Erronea diffusione, pubblicazione, comunicazione di dati personali
- Intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali
- Furto di archivi cartacei e/o digitali
- Accesso non autorizzato nel sistema informativo
- Azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali
- Smarrimento di dati personali (archiviati su supporti cartacei e digitali)
- Distruzione di dati personali (archiviati su supporti cartacei e digitali)
- Ecc.

4. *Procedura di gestione della violazione dei dati personali (data breach)*

Nel caso in cui un soggetto venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l’attuazione delle seguenti attività:

A. rilevazione della violazione dei dati personali

Il verificarsi di una violazione di dati personali può essere rilevato da qualsiasi soggetto interno (es. personale dipendente, liberi professionisti etc.) o da soggetti esterni (es. pazienti partecipanti agli studi, monitor, etc.).

B. comunicazione della violazione

Chiunque riceva notizia all'interno di FROM di una presunta violazione deve segnalare immediatamente quanto rilevato al Referente Privacy in prima istanza telefonicamente e successivamente per e-mail (privacy@fondazionefrom.it). Allegati alla presente istruzione i dati di contatto.

C. raccolta di informazioni sulla violazione

Il Referente Privacy raccoglie tutte le informazioni disponibili dalla persona / unità organizzativa che ha comunicato e rilevato la presunta violazione. Il Referente Privacy procede con una prima analisi della violazione di concerto con il Direttore Operativo e con il DPO.

D. compilazione sul MUA della prima parte del flusso di data breach fino a chiusura della sezione (step A-B-C)

E. compilazione da parte del DPO della seconda parte del Flusso, e valutazione della necessità di effettuare la comunicazione all'Autorità Garante

F. notifica del Titolare all'Autorità Garante della violazione subita, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche;

G. eventuale comunicazione del Titolare della violazione di dati personali all'interessato nel caso vi sia un rischio elevato. (Il documento per la segnalazione agli interessati potrà essere generato tramite il flusso MUA dei "data breach")

H. nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante sarà necessario registrare la violazione all'interno del sistema MUA, tramite lo svolgimento del Flusso di segnalazione di data breach, al fine di mantenere aggiornato il "Registro degli incidenti". Tale registro sarà reperibile all'interno del sistema nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - Data breach"

5. *Soggetti deputati ad avviare la procedura di gestione della violazione*

Il Flusso di gestione della violazione verrà avviata, tramite il sistema MUA, dal Referente Privacy o, in sua assenza dall'addetto alle registrazioni sul MUA (di seguito entrambi indicati con "incaricato") che agiranno secondo le indicazioni del Direttore Operativo.

Se la violazione riguarda un asset tecnologico-informatico, è opportuno che vengano coinvolti il Sistema Informatico Aziendale, o il referente per il sistema informativo, o la società esterna incaricata dell'assistenza informatica, al fine di valutare la portata della violazione e descrivere dettagliatamente l'accaduto. È inoltre opportuno che venga coinvolto il referente (interno o esterno) del servizio che ha subito la violazione.

6. *Modalità di avvio della procedura di gestione della violazione*

Fasi per la gestione del data breach:

1. comunicazione/segnalazione dell'evento che può comportare una violazione di dati all'incaricato individuato da FROM (vedi paragrafo precedente)
2. l'incaricato dell'inserimento sul MUA deve raccogliere, prima dell'avvio del flusso, tutte le informazioni necessarie
3. l'incaricato procede con l'accesso nominativo al sistema MUA attraverso l'indirizzo web <https://mua.secoges.com> e avvia il flusso "Privacy – Data breach" secondo le istruzioni descritte nell'allegato 1 "Descrizione del flusso data breach"
4. l'incaricato deve rispondere alle domande del questionario presenti in MUA relative a:
 - identificazione e descrizione dell'evento
 - misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione)
 - informazioni relative ai soggetti individuati per la gestione della procedura; se necessario dovrà farsi affiancare nella sua compilazione da coloro che sono in possesso delle informazioni
5. conclusa la compilazione del questionario l'incaricato chiude il flusso, completandolo e passando l'incarico al DPO.

La presente fase, a meno di giustificabili motivi condivisi con il DO e il DPO, deve essere conclusa entro 48 ore dal momento in cui il Titolare al trattamento, per mezzo del Referente Privacy o del Direttore Operativo è venuto a conoscenza della violazione di dati personali.
6. tramite il sistema MUA il DPO è incaricato dello svolgimento della seconda parte del flusso
7. il DPO riceve una mail dal sistema MUA che lo informa che è stato incaricato di svolgere la seconda parte del flusso
8. il DPO accede al sistema MUA attraverso l'indirizzo web <https://mua.secoges.com> dove trova evidenziato in rosso il pulsante "Attività da svolgere" e attiva il flusso attivo chiamato "Privacy – Data breach"
9. il DPO visualizza all'interno del sistema MUA le informazioni inserite durante la prima parte del flusso;
10. in base alle informazioni inserite il DPO valuta la necessità di fare comunicazione all'Autorità Garante e agli interessati e procede con la compilazione del questionario
11. il DPO procede fino alla chiusura del flusso in MUA:
 - 11.1. **Caso A: incidente da inserire nel registro incidenti**
 - 11.1.1. inserimento della violazione nel registro incidenti da parte dell'incaricato dell'inserimento sul MUA
 - 11.1.2. comunicazione da parte del DPO di chiusura della violazione alla mail privacy@fondazionefrom.it

11.2 Caso B (incidente da inserire nel registro incidenti e da notificare all'Autorità Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche)

11.2.1 Inserimento da parte dell'incaricato dell'inserimento sul MUA della violazione nel registro incidenti

11.2.2 Generazione da parte dell'incaricato dell'inserimento sul MUA del *fac-simile* di comunicazione di Data Breach

11.2.3 trasmissione da parte del DPO della comunicazione di chiusura della procedura alla mail privacy@fondazionefrom.it

11.2.4 acquisizione da parte dell'incaricato FROM, mediante download, del *fac-simile* di segnalazione di Data Breach all'Autorità Garante nel seguente modo:

- accedere alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach"
- posizionarsi sulla violazione/incidente inserito
- espandere la sezione "File allegati"
- cliccare sul documento da scaricare denominato "Modello di comunicazione al Garante-Data breach"
- la documentazione viene inviata, in automatico da sistema MUA, anche a mezzo mail agli indirizzi indicati durante lo svolgimento del flusso

11.2.5 L'Incaricato invia il *fac-simile* di comunicazione di Data Breach quale bozza di riferimento per la notifica della violazione dei dati personali all'Autorità Garante all'indirizzo privacy@fondazionefrom.it.

11.2.6 Il Referente Privacy, in collaborazione con il Direttore Operativo completa il modulo di notifica di violazione ricevuta dall'incaricato. Il contenuto del modulo di notifica viene condiviso con il DPO.

11.2.7 L'incaricato, su indicazione del Direttore Operativo, invia la notifica della violazione dei dati personali secondo le modalità operative previste dall'Autorità Garante e rese accessibili sul sito ufficiale dell'Autorità al link <https://servizi.gpdp.it/databreach/s/>.

11.2.8 Il modulo di notifica è caricato in MUA dall'Incaricato nel seguente modo:

- accedere alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach"
- posizionarsi sulla violazione/incidente inserito
- espandere la sezione "File allegati"
- cliccare su "Nuovo" e successivamente su "Seleziona il file da allegare"
- caricare il modulo di notifica della violazione dei dati personali e cliccare su "salva allegati"

11.3 Caso C (incidente da inserire nel registro incidenti, da notificare all'Autorità Garante e da comunicare agli interessati nel caso in cui la violazione comporti un rischio elevato per i diritti e la libertà delle persone fisiche)

11.3.1 inserimento della violazione nel registro degli incidenti e notifica all'Autorità Garante come da punti da 11.2.1 a 11.2.8

11.3.2 comunicazione della violazione di dati personali all'interessato

Il fac-simile del documento per la segnalazione agli interessati potrà essere generato dall'Incaricato tramite il flusso MUA "data breach".

L'Incaricato invia il *fac-simile* di modulo di comunicazione a privacy@fondazionefrom.it.

Il Referente Privacy completa il modulo di comunicazione e raccoglie le informazioni di contatto necessarie per l'invio agli interessati.

Il modulo di comunicazione agli interessati viene condiviso con il Direttore Operativo e con il DPO e viene deciso come procedere all'invio.

ALLEGATI:

1 - Descrizione del flusso data breach.

2 - Dati di contatto.