FEDERAZIONE ITALIANA SPORT DEL GHIACCIO

FEDERAZIONE SPORTIVA NAZIONALE RICONOSCIUTA DAL CONI

PROCEDURA DI DATA BREACH

(REDATTA AI SENSI E PER GLI EFFETTI DEGLI ARTT. 33 E 34 DEL REGOLAMENTO UE 2016/679)

29.10.2025

A) AMBITO DI APPLICAZIONE, SCOPI E DESTINATARI

Il presente documento è stato redatto dalla Federazione Italiana Sport del Ghiaccio n via Piranesi n. 46, Cap 20137, Milano (MI), CF 97016560159, P. IVA 05235981007 , indirizzo e-mail: info@fisg.it, allo scopo di illustrare i principi generali e la procedura da adottare per rispondere e mitigare le violazioni di dati personali per adempiere agli obblighi relativi alla notifica all'Autorità di controllo e ai singoli interessati così come previsto dagli artt. 33 e 34 del Regolamento UE n. 2016/679 (c.d. GDPR).

B) DEFINIZIONI

Ai sensi di quanto previsto dal Regolamento UE 2016/679 (c.d. GDPR):

1) per "*Trattamento*" si intende 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;
2) per "*Dato Personale*" si intende 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;
3) per "*Dati relativi alla Salute*" si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
4) per "*Categorie particolari di dati personali*" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
5) per "*Titolare del trattamento*" si intende 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
6) per "*Responsabile del trattamento*" si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare;
7) per "*Violazione dei dati personali*" si intende 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;
8) per "*Autorità di controllo*" si intende l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
9) per "*Autorità di controllo interessata*" si intende un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo.

C) SCOPO DELLA PROCEDURA

La funzione della procedura di Data breach è quella di fornire una risposta immediata ed efficace a qualsiasi sospetta e/o presunta e/o effettiva violazione dei dati personali trattati dal Titolare e subita da quest'ultimo.

Per violazione dei dati personali si intende ogni evento capace di mettere a rischio i dati trattati nell'ambito dell'attività svolta dal Titolare, tra cui: la divulgazione o l'accesso non autorizzati o accidentale di dati personali; la perdita di accesso o distruzione accidentale di dati personali; modifica non autorizzata o accidentale di dati personali.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

La funzione di coordinamento e di presidio dei processi connessi al protocollo di segnalazione e gestione delle violazioni di dati personali è affidata al Responsabile della procedura di Data breach.

D) LE FUNZIONI DEL RESPONSABILE DELLA PROCEDURA DI DATA BREACH

Il Responsabile della procedura di Data Breach (ove nominato) ha il compito di:

- supportare e presidiare il Titolare in materia di data breach;
- coordinarsi con il Responsabile per la protezione dei dati personali (RPD) e con i gruppi di lavoro in materia di sicurezza (se previsti);
- inviare la notifica della violazione dei dati personali al Garante per la protezione dei dati personali e ai soggetti interessati;
- compilare, curare e conservare il registro delle violazioni di dati.
- supportare il Titolare nella valutazione dei sistemi di rilevazioni delle violazioni dati;
-elaborare, verificare e aggiornare protocolli per la gestione del data breach;
-verificare nell'ipotesi di incidente di sicurezza informatica, se il rischio per gli interessati è probabile o improbabile e documentare e motivare la relativa valutazione;
- avvertire il Responsabile per la protezione dei dati personali (RPD) della violazione dei dati e aggiornare il medesimo sui relativi sviluppi;
- avvertire il Titolare della violazione dei dati;
- attivare, coordinare e documentare le indagini interne sugli incidenti di sicurezza che hanno comportato possibili violazioni di dati coordinandosi, per esempio, con i responsabili di settore (area personale, servizio ICT, amministratore di sistema, etc.);
- raccogliere gli elementi richiesti per la comunicazione della violazione all'Autorità Garante e ai soggetti interessati;
- comunicare le eventuali motivazioni per cui la notifica della segnalazione al Garante è avvenuta con ritardo;
-richiedere relazioni e report ai responsabili di settore (es. area personale, servizio ICT, etc.).

E) LA PROCEDURA DI RISPOSTA ALLE VIOLAZIONI DEI DATI PERSONALI

La procedura di risposta alle violazioni dei dati personali deve essere avviata quando si entra a conoscenza di una sospetta e/o presunta e/o effettiva violazione dei dati personali trattati.

Chi si accorge della suddetta violazione (Responsabile del trattamento, Responsabile della protezione dei dati personali, incaricati del trattamento dati, perdonale dipendente) ha l'obbligo di comunicarla immediatamente (e comunque, entro 24 ore lavorative

dalla conoscenza) al Titolare e/o al Responsabile della procedura di Data Breach, inviando una comunicazione via e-mail all'indirizzo del Titolare e/o al Responsabile della procedura di Data Breach: info@fisg.it

F) LA NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI DEL RESPONSABILE AL TITOLARE DEL TRATTAMENTO DEI DATI

Qualora la violazione dei dati personali o la sospetta violazione dei dati riguardasse i dati personali che vengono elaborati per conto di terzi, il Responsabile della procedura di Data breach o il Responsabile della Protezione dei dati (ove nominati) deve segnalare qualsiasi violazione dei dati personali al rispettivo Titolare/Titolari del trattamento dei dati senza indebito ritardo nelle modalità di comunicazione indicate dal/dai medesimo/i.

Il Responsabile della procedura di Data breach o il Responsabile della Protezione dei dati (ove nominati) invierà una notifica al Titolare che includerà quanto segue:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché delle 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 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 attenuarne i possibili effetti negativi.

Il Responsabile della procedura di Data breach registrerà la violazione dei dati nel Registro delle violazioni dei dati.

G) LA NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI AI SENSI DELL'ART. 33 DEL REGOLAMENTO UE 2016/679

Qualora si verifichi una violazione dei dati personali trattati – o vi sia il sospetto di una loro violazione – il Titolare del trattamento dei dati, il Responsabile della procedura di Data breach o il Responsabile della Protezione dei dati (ove nominati) dovrà attenersi alla seguente procedura:

1) Identificare un potenziale incidente di privacy ed eventuali eventi significativi;
2) Valutare l'importanza dell'incidente, raccogliendo tutte le informazioni aggiuntive necessarie e disponibili, prestando anche attenzione ai mezzi con cui è stata realizzata la violazione;
3) Accertare se si è verificato un incidente di sicurezza dei dati oppure se si è di fronte ad un falso allarme;
4) Se si accertata l'esistenza di un incidente di sicurezza dei dati, analizzare l'incidente e raccogliere il maggior numero di informazioni sulle modalità e sulle cause della violazione, stimando il rischio potenziale per i diritti e le libertà dell'interessato;
5) Identificare i mezzi di risposta più appropriati;
6) Aggiornare il Registro delle violazioni dei dati, descrivendo il tipo di violazione;
7) Stabilire se la violazione dei dati personali debba essere segnalata all'Autorità di controllo valuta;
8) Se è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà degli interessati, non è richiesta alcuna notifica. La violazione dei dati dovrà essere registrata dal Responsabile della procedura di Data Breach

nel Registro delle violazioni dei dati;

9) Il Titolare del trattamento o il Responsabile della procedura di Data Breach deve notificare la stessa violazione al Garante della protezione dei dati personali **senza indebito ritardo, e non oltre le 72 ore** se la violazione potrebbe avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali,
10) Oltre il termine di 72 ore, il Titolare del trattamento o il Responsabile della procedura di Data Breach deve specificare anche le ragioni del ritardo della notifica al Garante della protezione dei dati personali;
11) Redigere una relazione ex post avente ad oggetto la descrizione dell'incidente, i dati coinvolti, le misure di risposta adottate gestione dell'incidente da inserire nel Registro delle Violazioni.

Il Titolare o il Responsabile della procedura di Data breach (ove nominato) notificherà la violazione al Garante della protezione dei dati personali, includendo quanto segue:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché delle 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 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 attenuarne i possibili effetti negativi.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

H) LA COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO AI SENSI DELL'ART. 34 DEL REGOLAMENTO UE 2016/679

Il Titolare deve valutare se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

In caso affermativo, il Responsabile della procedura di Data breach o il Responsabile della Protezione dei dati (ove nominati) deve informare gli interessati senza ingiustificato ritardo inviando un'apposita comunicazione all'indirizzo e-mail da essi fornito.

La comunicazione agli interessati deve essere scritta in un linguaggio chiaro e semplice e deve contenere le seguenti informazioni:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché delle 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 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 attenuarne i possibili effetti negativi.

Se, a causa del numero di interessati o qualora non sia possibile identificare esattamente quali registrazioni siano state violate, è

sproporzionatamente difficile informare tutti i soggetti in questione, il Titolare dovrà adottare le misure necessarie per garantire che le persone interessate siano informate utilizzando canali appropriati e pubblicamente disponibili.
Qualora non sia possibile fornire le informazioni contestualmente, queste ultime possono anche essere comunicate in fasi successive senza ritardo.

Il **Titolare del trattamento è esonerato** dall'obbligo di comunicazione all'interessato se:

- ha messo in atto tutte le misure tecniche e organizzative adeguate di protezione e tali misure sono state applicate ai dati personali oggetto di violazione
- ha successivamente adottato le misure utili a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati.

I) INDICI DI VALUTAZIONE DELLA GRAVITA' DELLA VIOLAZIONE E DELLA NECESSITA' DI NOTIFICA AL GARANTE E AGLI INTERESSATI

La violazione è considerata di **bassa o media gravità** e NON DEVE essere notificata né al Garante della protezione dei dati, né agli interessati se:

- nessun individuo persona fisica è interessata dalla violazione;
- l'interessato potrebbe incontrare degli inconvenienti facilmente superabili, senza ulteriori fastidi (es. tempo trascorso a reinserire i dati);
- gli individui potrebbero incontrare notevoli disagi, che potranno però essere superati nonostante qualche difficoltà (es. costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, stress).

La violazione si considera di **alta gravità** e DEVE essere notificata al Garante della protezione dei dati se:

- gli individui possono incontrare conseguenze significative superabili, ma con gravi difficoltà (es. appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute).

La violazione è considerata **molto grave** e DEVE essere comunicata sia al Garante, sia all'interessato se:

- gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es. debiti finanziari, incapacità lavorativa, disturbi psicologici, morte).

J) IL REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI

Ai sensi dell'art. 33, paragrafo 5 del GDPR, il Titolare del trattamento è tenuto a documentare 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.
I campi del registro sono:

- data della violazione;
- natura e tipologia della violazione;
- descrizione della violazione;
- dati personali violati;
- numero di interessati colpiti/di registrazioni dei dati colpite;

- conseguenze della violazione;
- comunicazione della violazione agli interessati;
- misure adottate o proposte per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi;
- data di compimento delle azioni/misure.

Il soggetto preposto alla compilazione, cura e conservazione del registro delle violazioni di dati è il Responsabile della procedura di Data Breach.

Il presente registro deve essere conservato con diligenza e cura e può essere richiesto in sede ispettiva dall'Autorità di controllo.

L) <u>DISPOSIZIONI FINALI</u>

Presa visione del presente documento, gli autorizzati e/o i referenti interni confermano di aver correttamente recepito la presente procedura e le istruzioni impartite e si dichiarano competenti per la costante e diligente applicazione delle stesse.

La presente procedura di gestione del data breach è stata consegnata e/o inviata tramite posta elettronica agli autorizzati e/o ai referenti interni così come designati e le prescrizioni ivi contenute devono essere scrupolosamente osservate dai medesimi.

Gli autorizzati e/o i referenti interni sottoscrivendo la presente procedura o l'apposito registro di firma per avvenuta consegna e/o trasmissione, si impegnano, sin d'ora, ad adottare ogni futura istruzione che sarà impartita dal Titolare a seguito di aggiornamenti normativi e regolamentari o di modifiche tecnologiche o delle policy aziendali di trattamento di dati personali.

Milano,

Titolare del trattamento dei dati

FEDERAZIONE ITALIANA SPORT DEL GHIACCIO

ALLEGATO 1: ATTO DI NOMINA DEL RESPONSABILE DELLA PROCEDURA DI DATA BREACH

Lo scrivente Titolare del trattamento dei dati personali Federazione Italiana Sport del Ghiaccio, con sede legale in via Piranesi n. 46, Cap 20137, Milano (MI), CF 97016560159 | P. IVA 05235981007, indirizzo e-mail: info@fisg.it., atteso quanto rappresentato dagli artt. 33 e 34 del Regolamento UE 2016/679, con il presente atto provvede a nominare quale Responsabile della procedura di Data breach

il/la Sig./Sig.ra. ……

Il Responsabile della procedura di Data breach ha il compito di:

- supportare e presidiare il Titolare in materia di data breach;
- coordinarsi con il Responsabile per la protezione dei dati personali (RPD) e con i gruppi di lavoro in materia di sicurezza (se previsti);
- supportare il Titolare nella valutazione dei sistemi di rilevazioni delle violazioni dati;
- elaborare, verificare e aggiornare protocolli per la gestione del data breach;
- verificare nell'ipotesi di incidente di sicurezza informatica, se il rischio per gli interessati è probabile o improbabile e documentare e motivare la relativa valutazione;
- avvertire il Responsabile per la protezione dei dati personali (RPD) della violazione dei dati e aggiornare il medesimo sui relativi sviluppi;
- avvertire il Titolare della violazione dei dati;
- supportare il titolare nella valutazione della natura delle le violazioni di dati personali, accertando se le violazioni possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali;
- notificare la violazione dei dati personali trattati al Garante per la protezione dei dati personali entro 72 ore, motivando l'eventuale ritardo, tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/;
- comunicare la violazione dei dati personali all'interessato con un linguaggio semplice e chiaro;
- compilare, curare e conservare il Registro delle violazioni di dati.
- attivare, coordinare e documentare le indagini interne sugli incidenti di sicurezza che hanno comportato possibili violazioni di dati coordinandosi, per esempio, con i responsabili di settore (area personale, servizio ICT, amministratore di sistema, etc.);
- raccogliere gli elementi richiesti per la comunicazione della violazione all'Autorità Garante e ai soggetti interessati;
-richiedere relazioni e report ai responsabili di settore (es. area personale, servizio ICT, etc.);

ALLEGATO 2: COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO AI SENSI DELL'ART. 34 DEL REGOLAMENTO UE 2016/679.

Spettabile
……
……
……

OGGETTO: COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO AI SENSI DELL'ART. 34 DEL REGOLAMENTO UE 2016/679.

Gentile atleta/genitore/tutore/dipendente/volontario/cliente, la presente per informarLa che in data *[data]* abbiamo scoperto di avere subito una violazione dei dati personali che La riguardano i cui termini sono di seguito descritti.

1) DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE DEI DATI PERSONALI *(natura e descrizione violazione dei dati)*
2) DESCRIZIONE DELLE PROBABILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI PERSONALI
Reputiamo che la violazione di dati personali possa avere le seguenti conseguenze: *(elenco probabili conseguenze violazione)*
3) DESCRIZIONE DELLE MISURE ADOTTATE O PROPOSTE 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.
Le seguenti misure sono state adottate/saranno adottate per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi: *(elenco misure adottate/di cui si propone l'adozione)*
4) COMUNICAZIONE DEL NOME E DEI DATI DI CONTATTO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI O DI ALTRO PUNTO DI CONTATTO PRESSO CUI OTTENERE PIÙ INFORMAZIONI
Per qualsiasi informazione relativa alla violazione di dati, La preghiamo di contattare il nostro Responsabile della procedura di Data breach *(nome responsabile)* tramite e-mail (*indirizzo e-mail)* o per posta al seguente indirizzo *(indirizzo postale)* oppure al seguente recapito telefonico: *(recapito telefonico).*

Ciò premesso, il Titolare del trattamento rimane a Sua disposizione per fornire ulteriori chiarimenti e approfondimenti che si dovessero rendere necessari.

La ringraziamo per la sua collaborazione.

Con osservanza.