Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679)

Questo modulo, finalizzato a raccogliere informazioni per la notifica e la comunicazione di una violazione dei dati personali, deve essere utilizzato al solo fine di fornire al Responsabile della Protezione dei Dati (DPO) e/o al Consulente Privacy le informazioni necessari per valutare la violazione e, in particolare, per:

- valutare la necessità, o meno, di procedere alla notifica della violazione al Garante (art. 33 del RGPD);
- valutare la necessità, o meno, di procedere alla comunicazione della violazione agli interessati (art. 34 del RGPD);
- fornire al soggetto deputato le informazioni per la registrazione della violazione nel Registro delle Violazioni.

A tal fine si invita la Struttura a compilare le sezioni di seguito indicate in ogni sua parte. La notifica, sulla base della Convenzione nazionale, verrà inoltrata al Garante a cura del Responsabile della Protezione dei Dati sulla base delle informazioni fornite dal Titolare.

Si segnala che **nei campi liberi non ci sono limiti di caratteri: è però essenziale, per consentire la lettura del modulo, che lo stesso venga compilato informaticamente, e salvato in formato PDF** (non stampato in cartaceo e scansionato).

Si segnala che è possibile inviare al Garante ogni documento ritenuto opportuno ai fini della descrizione dei fatti. In tale caso si potranno inviare in allegato all'invio del presente modulo.

Si segnala che è essenziale e indispensabile che il presente modulo venga inviato nell'ambito dello stesso ticket aperto in esito alla comunicazione del data breach all'indirizzo privacy@cgil.it, oppure scrivendo nell'oggetto dell'email di invio il numero del ticket (es.: [CGIL-1726]).

Il modulo non può essere inoltrato al Garante in quanto, ai fini della notifica, può procedersi solo attraverso la procedura prevista e raggiungibile al link https://servizi.gpdp.it/databreach/s/scelta-auth.

Maggiori informazioni sono disponibili sul sito istituzionale del Garante Privacy (https://servizi.gpdp.it/databreach/s/) o, comunque, possono essere chieste al DPO scrivendo all'indirizzo privacy@cgil.it avendo cura di rispondere alla stessa email ricevuta dal DPO stesso oppure inviando l'email inserendo nell'oggetto il numero del ticket (nel formato "CGIL-0000").

1. Struttura presso la quale è avvenuta la violazione

La compilazione di questa sezione è obbligatoria. In mancanza non è possibile per il DPO avere le informazioni utili per procedere alla notifica.

Indicare le informazioni relative alla struttura presso la quale è avvenuta la violazione (è necessario indicare, salvo ove diversamente richiesto, i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Si segnala che, in ogni caso, il soggetto notificante della violazione, ai sensi dell'accordo di contitolarità della Confederazione, è individuato nel Centro Regolatore Nazionale presso il quale è avvenuto (se, appunto, verificatosi presso una sede nazionale) oppure nel Centro Regolatore regionale nell'ambito del quale territorio si è verificato il data breach. La struttura qui individuata verrà indicata nell'atto di notifica come "ulteriore soggetto coinvolto", segnatamente come contitolare del trattamento, salvo successive emergenze.

Denominazione[1]

Codice Fiscale[2]

CAP

Comune[3]

Indirizzo[4]

Telefono[5]

E-mail[6]

PEC[7]

Segretario Generale[8]

Referente[9]

Recapiti Referente[10]

1 Indicare il nominativo della Struttura CGIL nell'ambito della quale è avvenuto il data breach, ad es. Camera del Lavoro di Velletri, FILCAMS di Vicenza, SPI Emilia-Romagna, FLAI Nazionale, ecc…)

2 Indicare il codice fiscale della Struttura CGIL indicata al punto precedente

3 Indicare il comune (non la frazione) in cui ha sede la Struttura CGIL indicata al primo punto

4 Indicare la sede principale (non quella in cui è avvenuta la violazione) della Struttura CGIL indicata al primo punto

5 Indicare il numero di telefono presso il quale sia reperibile un soggetto che abbia informazioni utili ai fini del data breach. Non indicare un numero di telefono generico (tipo il centralino) ma il numero di un soggetto che potrebbe essere contattato dal Garante e/o dal DPO

6 Indicare come in nota 5.

7 Indicare la PEC della Struttura CGIL indicata al primo punto, se esistente. Non è un dato obbligatorio

8 Indicare cognome e nome del Segretario Generale attuale della Struttura CGIL indicata al primo punto

9 Indicare cognome e nome di una persona a conoscenza del data breach, che potrebbe essere contattata dal DPO

10 Indicare i recapiti del Referente, numero di telefono, indirizzo email, o entrambi

2. Ulteriori soggetti coinvolti nel trattamento

La compilazione di questa sezione non è obbligatoria: potrebbero non esserci ulteriori soggetti coinvolti.
In questa sezione è necessario inserire i dati di **eventuali** altri soggetti coinvolti nel *data breach* (ad es. società informatiche che gestiscono la piattaforma dove è avvenuta la violazione, eventuali altre strutture CGIL coinvolte, soggetto terzi che gestivano e/o trattavano dati per conto della Struttura indicata al punto 1, ecc..).

Denominazione[11]

Codice Fiscale[12]

CAP

Comune[13]

Indirizzo[14]

Telefono[15]

E-mail[16]

PEC[17]

Segretario Generale[18]

Referente[19]

Recapiti Referente[20]

11 Indicare il nominativo della Struttura CGIL nell'ambito della quale è avvenuto il data breach, ad es. Camera del Lavoro di Velletri, FILCAMS di Vicenza, SPI Emilia-Romagna, FLAI Nazionale, ecc…)
12 Indicare il codice fiscale della Struttura CGIL indicata al punto precedente
13 Indicare il comune (non la frazione) in cui ha sede la Struttura CGIL indicata al primo punto
14 Indicare la sede principale (non quella in cui è avvenuta la violazione) della Struttura CGIL indicata al primo punto
15 Indicare il numero di telefono presso il quale sia reperibile un soggetto che abbia informazioni utili ai fini del data breach. Non indicare un numero di telefono generico (tipo il centralino) ma il numero di un soggetto che potrebbe essere contattato dal Garante e/o dal DPO
16 Indicare come in nota 5.
17 Indicare la PEC della Struttura CGIL indicata al primo punto, se esistente. Non è un dato obbligatorio
18 Indicare cognome e nome del Segretario Generale attuale della Struttura CGIL indicata al primo punto
19 Indicare cognome e nome di una persona a conoscenza del data breach, che potrebbe essere contattata dal DPO
20 Indicare i recapiti del Referente, numero di telefono, indirizzo email, o entrambi

3. Informazioni sulla violazione

In questa sezione è necessario fornire la maggior parte delle indicazioni necessarie per poter ricostruire quanto accaduto e le modalità in cui si è verificato il data breach.

3.1. Momento in cui è avvenuta la violazione

☐ Il (indicare di seguito la data)

☐ Dal (indicare di seguito quando è iniziata la violazione)

☐ In un tempo non ancora determinato, indicare di seguito ulteriori specifiche:

3.2. Modalità con la quale il titolare è venuto a conoscenza della violazione

3.3. Momento in cui il titolare è venuto a conoscenza della violazione

Data **Ora**

3.4. Motivi del ritardo[21]:

3.5. Descrizione della violazione[22]:

21 Compilare solo se la data di cui al punto precedente è anteriore alle 72 ore.

22 Descrivere analiticamente cosa è acceduto, ovvero come è avvenuto il data breach, dove, ad opera di chi, attraverso quali modalità.

3.6. Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione[23]:

3.7. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti[24]:

3.8. Categorie di interessati coinvolti nella violazione

- ☐ Iscritti
- ☐ Lavoratori non iscritti
- ☐ Soggetti che hanno contatti con la Struttura
- ☐ Utenti di altri soggetti (CAAF, Inca, ecc.)
- ☐ Dipendenti
- ☐ Collaboratori e/o Volontari
- ☐ Soggetti vulnerabili (anziali, disabili, ecc.)
- ☐ Minori
- ☐ Soggetti dirigenti (componenti di segreteria, ecc.)
- ☐ Altri soggetti (specificare di seguito):

23 Paragrafo da compilare solo se trattasi di violazione di natura informatica. Nel caso, indicare specificamente il sistema informativo, il software, la piattaforma attraverso la quale è avvenuto il data breach.

24 Indicare specificamente le misure che erano state adottate per evitare la violazione poi in realtà verificatasi. Se esistente, allegare la valuatazione di impatto.

3.9. Numero (anche approssimativo) di interessati coinvolti nella violazione:

3.10. Categorie di dati personali oggetto di violazione[25]:

- ☐ Dati anagrafici (nome, cognome, genere, data, luogo nascita
- ☐ Dati di contatto (indirizzo, email, numero telefono)
- ☐ Dati di accesso e di identificazione (userId, password, altro)
- ☐ Dati di pagamento (n. conto corrente, carta di credito, ecc…)
- ☐ Dati fornitura servizi comunicazione elettronica (traffico tele
- ☐ Dati relativi a condanne penali, reati o a misure sicurezza
- ☐ Dati che rivelano l'appartenenza sindacale
- ☐ Dati genetici
- ☐ Categorie non ancora determinate (specificare):
- ☐ Dati di profilazione
- ☐ Dati relativi a documenti di identificazione/riconoscimento
- ☐ Dati relativi all'ubicazione
- ☐ Dati che rivelano l'origine razziale o etnica
- ☐ Dati che rivelano le opinioni politiche
- ☐ Dati che rivelano le convinzioni religiose o filosofiche
- ☐ Dati relativi a vita e orientamento sessuale
- ☐ Dati relativi alla salute
- ☐ Altre categorie (specificare):

3.11. Numero (anche approssimativo) di registrazioni[26] dei dati personali oggetto di violazione

25 Laddove la violazione abbia ad oggetto dati personali distingi per interessato, nel campo libero descrivere nel dettaglio le categorie di dati personali e distinguerli per ciascuna categoria di interessati.

26 Ad esempio numero di deleghe, tessere, fatture, ordini, referti, immagini, record di un database o numero di transazioni.

4. Misure adottate a seguito della violazione

4.1. *Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati[27]:*

4.2. *Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future[28]* (c.d. azioni di miglioramento)*:*

27 In questo paragrafo è necessario evidenziare cosa si è fatto per tentare di porre rimedio a quanto accaduto o per mitigare il danno subito o subendo dalla violazione, sia per la Struttura sia per le persone I cui dati sono stati violati. Si segnala che, in ogni caso, eventuali indicazioni potranno essere suggerite anche dal DPO.

28 In questo paragrafo è necessario evidenziare quali misure di sicurezza verranno adottate, in futuro, per evitare che si verifichino nuovamente eventi simili. Si segnala che, in ogni caso, eventuali misure potranno essere suggerite anche dal DPO.

5. Comunicazione della violazione agli interessati

Si evidenzia che, 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 è tendenzialmente tenuto a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo.
Di seguito vengono richieste le informazioni necessarie per valutare se ed in che misura sia da ritenersi necessaria la comunicazione agli interessati.
In esito alla valutazione del *data breach* il DPO comunicherà alla Struttura di cui sopra, e al relativo Centro Regolatore, il proprio parere in ordine all'obbligo e, eventualmente, alle modalità attraverso le quali procedere alla comunicazione stessa.

5.1. Con riferimento alla specifica violazione e al trattamento svolto:

5.1.1. La struttura, **prima** del verificarsi del *data breach* in analisi, aveva messo in atto misure tecniche e/o organizzative che rendevano i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura dell'HD, criptazione dei dati, ecc.)?

☐ SI (compilare la casella che segue) ☐ NO

In caso di risposta affermativa, indicare quali misure erano state applicate:

5.1.2. La struttura, **dopo** il verificarsi del *data breach*, ha applicato misure finalizzate a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (con riferimento, quindi, agli specifici dati oggetto del *data breach*)?

☐ SI (compilare la casella che segue) ☐ NO

In caso di risposta affermativa, indicare quali misure sono state applicate:

5.1.2. La struttura ritiene che la comunicazione del *data breach* a tutti i singoli interessati comporti sforzi sproporzionati o eccessivi[29]?

☐ SI (compilare la casella che segue) ☐ NO

In caso di risposta affermativa, indicarne la ragione:

5.2. Numero di interessati a cui potrà essere comunicata la violazione

La comunicazione verrà inviata a n. ☐ interessati[30].

Eventuali note:

5.3. Canale che si propone di utilizzare per la comunicazione agli interessati

La comunicazione agli interessati potrà essere inviata a mezzo:

Eventuali note:

29 Si segnala che in caso di risposta affermativa, laddove si ritenga di convenire, dovrà comunque essere disposta una comunicazione impersonale di pubblico dominio (es. pubblicazione nel sito istituzionale della struttura, pubblicazione su un quotidiano, ecc.). In ogni caso si segnala altresì che la comunicazione agli interessati può essere inviata anche a mezzo sms e/o email.

30 Può essere indicato anche un numero approssimativo, se non individuato con precisione.

6. Altre informazioni

6.1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[31]?

☐ SI (compilare la casella che segue) ☐ NO

In caso di risposta affermativa, indicare l'autorità alla quale è stata fatta la notifica e la norma di riferimento:

6.2. È stata effettuata la segnalazione[32] all'autorità giudiziaria o di polizia?

☐ SI (allegare la segnalazione) ☐ NO

31 Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

32 Denuncia, Esposto, Querela. Nel caso sia stata fatta è necessario allegarne copia.