TEACH FOR ITALY
Insegnare per L'Italia

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH) AI SENSI DEL REGOLAMENTO UE n. 2016/679

1) PREMESSE

Teach For Italy - Insegnare per l'Italia (di seguito "**Associazione**"), ai sensi del Regolamento (UE) n. 2016/679 (di seguito, per brevità, anche il "**Regolamento**"), è tenuta a garantire la sicurezza dei dati personali trattati nell'ambito delle proprie attività, nonché ad agire senza ingiustificato ritardo nel caso si verifichi una violazione dei dati personali.

È di fondamentale importanza predisporre e implementare policy e procedure contenenti le azioni da attuare in caso si verifichino violazioni dei dati personali concrete, potenziali o anche solo sospette.

2) SCOPO

La presente procedura (di seguito la "**Procedura**") ha lo scopo di fornire indicazioni pratiche sulla gestione delle violazioni di dati personali (di seguito "**Violazioni"** o **"Data Breach"**) trattati dall'**Associazione**, sia in qualità di Titolare del trattamento che di Responsabile del trattamento.

3) DESTINATARI E AMBITO DI APPLICAZIONE

La **Procedura** è rivolta ai lavoratori dipendenti, ai collaboratori e/o comunque a tutti i soggetti che, a qualsiasi titolo, prescindendo dal tipo di rapporto intercorrente con l'**Associazione**, trattino o comunque abbiano accesso per conto della stessa ai dati personali (di seguito i "**Destinatari**").

La **Procedura** è resa nota a tutti i **Destinatari** mediante modalità che ne garantiscono l'effettiva conoscibilità e comprensione, anche attraverso attività informative e formative.

È fatto obbligo a tutti i **Destinatari** di conoscere la **Procedura** e di conformarsi alle regole di comportamento ivi previste.

I comportamenti tenuti dai lavoratori dipendenti in violazione della **Procedura** e delle regole di comportamento ivi descritte sono considerati illeciti disciplinari.

I comportamenti posti in essere da collaboratori in violazione della **Procedura** e delle regole di comportamento ivi descritte costituiscono inadempimento contrattuale e potranno determinare la risoluzione del rapporto, fatta salva l'eventuale richiesta di risarcimento del danno, qualora dal comportamento sia derivato un danno concreto per l'**Associazione**.

4) NORMATIVA DI RIFERIMENTO

Art. 33 Regolamento: Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 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 dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la 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;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere 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.

4. 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.

5. 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. 34 Regolamento: Comunicazione di una violazione dei dati personali all'interessato

1. 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.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

5) DEFINIZIONI

Dato personale

Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "**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.

Tra i dati personali, ci sono i dati c.d. "particolari", ossia quei dati che rivelano l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati relativi alla vita sessuale o all'orientamento sessuale della persona.

Trattamento

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.

Interessati

Per interessati si intendono coloro ai quali di dati personali si riferiscono.

Destinatari

Per Destinatari si intendono i lavoratori dipendenti, i collaboratori e/o comunque tutti i soggetti che, a qualsiasi titolo, prescindendo dal tipo di rapporto intercorrente con l' **Associazione**, trattino o comunque abbiano accesso per conto della stessa ai dati personali.

Violazione o **Data Breach**

Per Violazione o Data Breach si intende una qualsiasi infrazione alla sicurezza dei dati che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati.

A titolo meramente esemplificativo, le Violazioni possono consistere in o derivare da:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- accesso abusivo;
- pirateria informatica;
- banche dati distrutte o alterate senza autorizzazione del relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (es. forzatura di porte e finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di laptop, devices o attrezzature informatiche aziendali;
- invio di email contenenti dati personali al destinatario sbagliato.

Referente Data Breach

Il soggetto, interno all' **Associazione**, individuato e designato dall' **Associazione** per la gestione delle **Violazioni**. La figura del Referente Data Breach può coincidere con quella del Referente Privacy designato dall'**Associazione**.

Referente Privacy

Il soggetto incaricato dall' **Associazione** di gestire gli adempimenti privacy su istruzioni dell'**Associazione** stessa. Il Referente Privacy può assumere anche il ruolo di **Referente Data Breach**.

Registro delle Violazioni

È il registro ove devono essere documentate, secondo le modalità previste nella **Procedura**, tutte le **Violazioni**, concrete, potenziali o anche solo sospette.

Il registro è tenuto dall' **Associazione** e conservato a cura del **Referente Data Breach**.

6) COME GESTIRE LE VIOLAZIONI

Le **Violazioni**, se non sono affrontate e gestite in modo adeguato, possono provocare danni agli **Interessati** (pregiudizio alla reputazione, perdite finanziarie, discriminazioni, usurpazioni di identità ecc.).

Al fine di minimizzarne l'impatto e di prevenire la ripetizione di eventi analoghi, è necessario affrontare la **Violazione** - sia essa concreta, potenziale o sospetta - in modo immediato e corretto.

Per gestire la **Violazione** è necessario seguire la **Procedura**, che si articola nelle seguenti fasi.

Fase 1 - SEGNALAZIONE e RACCOLTA DI INFORMAZIONI

a) Segnalazione

I Destinatari, non appena vengono a conoscenza di una **Violazione**, concreta, potenziale o anche solo sospetta, indipendentemente dal fatto di esserne o meno responsabili, ne devono dare immediata notizia all' **Associazione** e per essa al **Referente Data Breach**, a mezzo e-mail all'indirizzo apastorelli@teachforitaly.org *[indicare l'indirizzo e-mail del Referente Data Breach]*, ovvero utilizzando le vie brevi (per telefono o di persona).

b) Raccolta di informazioni

Appena ricevuta la segnalazione, il **Referente Data Breach** informa l'**Associazione** e, nello specifico, il Presidente del Consiglio Direttivo Silvia Pulino, e raccoglie dal soggetto che ha effettuato la segnalazione e da tutti i **Destinatari** coinvolti, tenuti a collaborare, le informazioni sulla presunta **Violazione** e procede alla compilazione del "*Modulo di rilevazione Data Breach*" (allegato *sub* A).

› Qualora la **Violazione** riguardi dati contenuti in un sistema informatico, il **Referente Data Breach** coinvolge in tutte le fasi della **Procedura** anche il Responsabile IT o un suo delegato.

›

› Il **Referente Data Breach** informa, inoltre, della **Violazione** il **Referente Privacy**, se diverso, fornendogli copia del Modulo sopra indicato.

›

› Se, analizzate tutte le informazioni raccolte, si esclude la sussistenza di un **Data Breach** (perché, ad esempio, i dati persi sono criptati e non possono essere violati utilizzando i mezzi tecnici disponibili e l'Associazione ha realizzato adeguati back up dei dati oppure è stato smarrito un pc ma non vi sono presenti dati personali), la **Procedura** termina con la compilazione del "*Modulo di rilevazione Data Breach*", che deve essere adeguatamente conservato dall' **Associazione** a cura del **Referente Data Breach**.

›

› Se, analizzate tutte le informazioni raccolte, è confermata la sussistenza di un **Data Breach**, il **Referente Data Breach**, previa consultazione con l'**Associazione** e dietro indicazioni di questa, compila il **Registro delle Violazioni,** ove vengono inserite le ulteriori informazioni ottenute all'esito di ogni fase della **Procedura** e si procede con la fase 2.

Fase 2 - ANALISI DEL RISCHIO

› A seguito della compilazione del "*Modulo di rilevazione Data Breach*", l'**Associazione**, insieme al **Referente Data Breach**, al **Referente Privacy**, se diverso, analizza tutte le informazioni raccolte e inizia a redigere la "*Scheda di valutazione del rischio*" (allegato *sub* B).

›

› Per valutare il livello di rischio, si prendono in considerazione i seguenti aspetti:

- tipo di **Violazione** (riservatezza, integrità e disponibilità dei dati);
- tipologia di **Dati personali** coinvolti;
- categoria di **Interessati** coinvolti;

- facilità di identificazione degli **Interessati**;
- numero degli **Interessati** identificabili coinvolti;
- possibili conseguenze della violazione sugli **Interessati**;
- potenziali effetti negativi sugli **Interessati**.

›

› L'**Associazione**, insieme al **Referente Data Breach**, al **Referente Privacy**, se diverso, valutano se esistono azioni/misure che possano limitare i danni derivati o che potrebbero derivare dal **Data Breach** (ad es. riparazione fisica di strumentazione, utilizzo dei file di back up per recuperare dati persi o danneggiati, isolamento o chiusura di un settore compromesso della rete, cambio dei codici di accesso, ecc.).

›

› Una volta individuate le misure correttive, l'**Associazione** o, su indicazione di questa, il **Referente Privacy** comunica le azioni da attuare e le misure da adottare ai **Destinatari** interni ed esterni coinvolti - o che potrebbero essere coinvolti - nei processi aziendali in cui si è verificata la **Violazione** o che hanno subito conseguenze in seguito alla **Violazione** nonché, se necessario, a tutta la struttura organizzativa. L'**Associazione** o, su indicazione di questa, il **Referente Privacy** indica altresì i tempi di attuazione.

›

› L'**Associazione**, insieme al **Referente Data Breach**, al **Referente Privacy,** se diverso, devono poi valutare se, anche alla luce delle misure correttive adottate, dalla **Violazione** possa derivare un rischio per i diritti e le libertà delle persone. Detti rischi, aventi probabilità e gravità diverse, possono derivare da "*trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine*

di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati" (Considerando 75 Regolamento).

› All'esito di detta valutazione, il **rischio per i diritti e le libertà delle persone fisiche** potrà essere trascurabile, basso, medio o alto.

› In caso di rischio **trascurabile**, il **Referente Data Breach,** previa consultazione con l'**Associazione** e dietro indicazioni di questa, completa l'annotazione della **Violazione** nel **Registro delle violazioni**.

› In caso di rischio **basso, medio o alto**, si procederà come previsto nella fase 3.

Fase 3 - ADEMPIMENTI SUCCESSIVI ALL'ANALISI DEL RISCHIO

› In caso di rischio **basso o medio**, il **Referente Data Breach,** previa consultazione con l'**Associazione** e dietro indicazioni di questa, completa l'annotazione della **Violazione** nel **Registro delle violazioni**.

› Entro 72 ore dal momento in cui si è avuta conoscenza della violazione, l'**Associazione** effettua la notifica al Garante, utilizzando il "*Modulo di Notifica*" (allegato *sub* C). La notifica va effettuata al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it.

Se la notifica è effettuata oltre il predetto temine di 72 ore, questa deve essere corredata dalle ragioni del ritardo. Qualora e nella misura in cui non sia possibile fornire al Garante tutte le informazioni indicate nel Modulo di Notifica, queste devono essere fornite in un momento successivo, senza ingiustificati ritardi (c.d. notifica a fasi).

› In caso di rischio **elevato**, il **Referente Data Breach** previa consultazione con l'**Associazione** e dietro indicazioni di questa, completa l'annotazione della **Violazione** nel **Registro delle violazioni**. L'**Associazione** effettua la notifica al Garante per la protezione dei dati personali come sopra indicato e, senza ingiustificato ritardo, comunica la **Violazione** agli **Interessati** coinvolti.

› La comunicazione deve descrivere con linguaggio semplice e chiaro la natura della Violazione e contenere almeno le seguenti informazioni: nome e dati di contatto del **DPO** se nominato o di altro punto di contatto presso cui ottenere più informazioni, le probabili conseguenze della **Violazione**, le misure adottate o

di cui si propone l'adozione per porre rimedio alla **Violazione** o per attenuarne i possibili effetti negativi.

› La comunicazione deve essere effettuata nella lingua madre degli **Interessati** coinvolti e, qualora necessario, in inglese.

› La comunicazione è effettuata personalmente all'**Interessato**, preferendo modalità di messaggistica diretta quali SMS, e-mail, lettera, se tali indirizzi sono a disposizione dell'**Associazione**. Ove ciò non fosse possibile o nel caso in cui la comunicazione diretta richiedesse sforzi sproporzionati, deve essere effettuata una comunicazione pubblica, quale ad esempio la pubblicazione sul sito web dell'**Associazione** di un messaggio contenuto in un banner che sia facilmente individuabile.

La modalità di comunicazione agli **Interessati** sarà scelta dall'**Associazione** in considerazione del numero e delle categorie di **Interessati**.

7) ATTUAZIONE E CONTROLLO

L'**Associazione** si impegna a garantire la diffusione della **Procedura**, mediante la distribuzione a tutti i **Destinatari**.

Promuove, inoltre, iniziative periodiche di formazione sul suo contenuto, verificandone, inoltre, l'integrale rispetto ed osservanza.

8) ALLEGATI

A) Modulo di rilevazione Data Breach

B) Scheda di valutazione del rischio

C) Modulo di Notifica al Garante per la protezione dei dati personali

D) Schema riassuntivo

9) APPENDICI

A) Data Breach di dati trattati in qualità di Responsabile ex art. 28 Regolamento

B) Data Breach di dati trattati da un Responsabile ex art. 28 Regolamento

› Roma, (data) _____

TEACH FOR ITALY
Insegnare per L'Italia

›

Teach For Italy - Insegnare per l'Italia

APPENDICE A)

DATA BREACH DI DATI TRATTATI IN QUALITA' DI RESPONSABILE

Se la **Violazione** ha ad oggetto dati trattati dall'**Associazione** in qualità di Responsabile del trattamento ex art. 28 Regolamento, l'**Associazione** ne dà notizia al Titolare nei tempi e nelle forme previsti dal contratto tra loro stipulato (il Contratto) o, in mancanza, entro le 24 ore.

Nel frattempo, l'**Associazione** procedere con gli adempimenti della FASE 1 e FASE 2 della **Procedura**, con esclusione della compilazione del **Registro delle violazioni**.

Salve diverse indicazioni previste dal Contratto, terminata la FASE 2, l'**Associazione** informa il Titolare dell'esito delle verifiche e valutazioni e gli consegna gli Allegati A e B compilati e comunque tutta la documentazione utile per permettergli, se necessario, di notificare la **Violazione** all'Autorità di Controllo competente e di comunicarla, se del caso, agli **Interessati**, nei termini e con le modalità indicati agli art. 33 e 34 del Regolamento. Ciò, avendo cura di verificare che il Titolare vi provveda.

APPENDICE B)

DATA BREACH DI DATI TRATTATI DA UN RESPONSABILE

Salve diverse indicazioni previste dal Contratto, se l'Associazione ha notizia di una **Violazione** avente ad oggetto dati trattati per conto dell'Associazione da un Responsabile del trattamento ex art. 28 Regolamento, si attiva per ottenere dal Responsabile tutte le informazioni e la documentazione utile per procedere, se necessario, con la notifica della **Violazione** all'Autorità di Controllo competente e con la comunicazione, se del caso, agli **Interessati,** nei termini e con le modalità indicati agli art. 33 e 34 del Regolamento.