Manuale Operativo per l'adeguamento al GDPR (Reg. Ue 2016/679) per Istituti Scolastici e Comprensivi	

Manuale Operativo per l'adeguamento al GDPR per Istituti Scolastici e Comprensivi

Nome documento:	Manuale Operativo per l'adeguamento al GDPR per Istituti Scolastici e Comprensivi
Codice documento:	GDPR Scuole - Manuale Adeguamento GDPR Ver 1-0.doc
Nome file:	GDPR Scuole - Manuale Adeguamento GDPR Ver 1-0.doc
Stato documento:	Definitivo
Autore:	Dott. Giancarlo Favero
Versione:	1.0
Data creazione:	2 maggio 2018
Data ultimo aggiornamento	11 giugno 2018

Manuale Operativo per l'adeguamento al GDPR (Reg. Ue 2016/679) per Istituti Scolastici e Comprensivi	

Indice

Manuale Operativo per l'adeguamento al GDPR (Reg. Ue 2016/679) per Istituti Scolastici e Comprensivi	

Art. 1 - Obiettivo del presente documento

Obiettivo del presente documento è fornire agli Istituti Scolastici e Comprensivi uno strumento chiaro e semplice per adeguarsi al GDPR.

L'utente principale di questo manuale operativo può essere il Dirigente Scolastico o il D.S.G.A., oppure chi in seno all'Istituto si occupi dell'adeguamento al GDPR.

La presente guida è predisposta da Data Security (www.datasecurity.it), divisione sicurezza di Swisstech S.r.l., azienda leader da trent'anni in Italia nei servizi di sicurezza e protezione dei dati personali per la Pubblica Amministrazione, la Sanità e la grande industria.

Passo 1: designazione del Responsabile della protezione dei dati

Il Responsabile della protezione dei dati è una delle più significative novità introdotte dal GDPR. In generale si tratta di un soggetto esterno, poiché deve possedere adeguate competenze ed esperienza che difficilmente si possono reperire all'interno dell'Ente.

Per designare il Responsabile della protezione dei dati bisogna prendere il documento ***Modello A – Schema di designazione RPD-DPO*** allegato, mettere nell'intestazione i dati dell'Ente e sostituire ad ***Ente X*** i dati dell'Istituto. Il

documento dovrà essere firmato dal Legale Rappresentante dell'Ente, che di norma è il Dirigente Scolastico.

Passo 2: Pubblicare i dati di contatto del Responsabile della protezione dei dati sul sito web dell'Ente e in bacheca

Dopo aver designato con atto scritto il Responsabile della protezione dei dati (detto anche per brevità ***DPO***, dall'inglese ***Data Protection Officer***), è necessario pubblicare sul sito web dell'Ente i dati di contatto del DPO.

I dati di contatto del DPO Da pubblicare si trovano in calce al succitato ***Modello A – Schema di designazione RPD-DPO***, che per comodità si riportano di seguito:

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati designato ai sensi dell'art. 37 del Regolamento UE 2016/679 è la Ditta Swisstech S.r.l. nella persona del Dott. Giancarlo Favero, responsabile di Data Security, (www.datasecurity.it), divisione sicurezza di Swisstech S.r.l.

Ai sensi dell'art. 38 comma 4 del GDPR gli interessati (dipendenti, genitori, alunni, cittadini, fornitori etc.) possono contattare senza formalità il Responsabile della protezione dei dati Dott. Giancarlo Favero per tutte le questioni relative al trattamento dei loro dati personali dati personali e all'esercizio dei loro diritti.

Il Responsabile della protezione dei dati personali può essere contattato al 335-5950674, oppure alla mail dpo@datasecurity.it.

.

Di solito i dati di contatto del DPO vengono pubblicati all'interno della sezione ***Privacy*** del sito web, se esistente (oppure allo scopo si può valutare di crearne una), oppure possono essere pubblicati all'interno della sezione ***Amministrazione Trasparente***. E' importante comunque porre attenzione al fatto che la pagina esatta di pubblicazione sia comunicata al Garante per la protezione dei dati personali, come spiegato nel prossimo passo.

Passo 3: Comunicare i dati di contatto del Responsabile della protezione dei dati al Garante per la protezione dei dati personali

Ora è necessario comunicare i dati di contatto del Responsabile della protezione dei dati al Garante per le protezione dei dati personali, cosa che si può fare solamente con la procedura online disponibile sul sito del garante, al seguente link:

https://servizi.gpdp.it/comunicazione-rpd/

Nella sezione A bisogna introdurre i dati di chi materialmente esegue la comunicazione; nella sezione B bisogna introdurre i dati del titolare del trattamento dei dati, che è l'Ente nel suo complesso, avendo cura di selezionare il secondo bottone, cioè quello relativo a soggetto censito nell'indice dei domicili digitali delle pubbliche amministrazioni:

o *Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestoridi pubblici servizi (www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)*

Nella sezione C bisogna inserire i dati del Responsabile della protezione dei dati, prendendoli dal

Modello B allegato (**Modello B – Dati per comunicazione DPO al Garante**).

Passo 4: Diramare la comunicazione relativa alle violazioni dei dati a tutti i dipendenti

Una significativa novità introdotta dal GDPR è l'obbligo di notificare al Garante per la protezione dei dati personali entro 72 ore alcune tipologie di violazioni dei dati.

E' pertanto necessario che tutti i dipendenti sappiano precisamente cos'è una violazione dei dati, come può concretizzarsi, e che devono prontamente comunicarla ad un soggetto interno all'Ente opportunamente designato e al DPO, che si farà carico di effettuare tutte le valutazioni del caso. Per fare questo si deve utilizzare il documento

GDPR Scuole - DOC001 – Comunicazione Data Breach per Comuni

allegato, personalizzarlo con i dati dell'Ente, farlo firmare dal Dirigente Scolastico, protocollarlo ed inviarlo a tutti i dipendenti e collaboratori (es. stagisti, interinali etc.).

Passo 5: Istituire il Registro delle violazioni dei dati e degli incidenti informatici

Strettamente collegata al punto precedente, è l'attività che consiste nell'istituire e tenere regolarmente aggiornato Registro delle violazioni dei dati e degli incidenti informatici.

Per fare questo bisogna prendere il documento

GDPR Scuole – DOC002 – Registro delle Violazioni dei Dati

personalizzarlo con i dati dell'Ente e tenerlo regolarmente aggiornato, di concerto con il DPO.

Passo 6: Notificare una violazione dei dati personali

Nel caso si dovesse effettivamente verificare una violazione dei dati personali, occorre avvertire immediatamente il Responsabile della protezione dei dati al numero 335-5950674 e alla mail dpo@datasecurity.it, che se del caso provvederà ad effettuare la notificazione al garante, di concerto con il Referente dell'Ente, e nel caso la cosa sia richiesta, provvederà a darne comunicazione agli interessati.

Passo 7: Istituire il Modello Organizzativo e le Disposizioni Operative per l'Adeguamento al GDPR e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni Secondo gli Standard ISO 27001 e 27002

Questo costituisce uno dei punti chiave dell'adeguamento il GDPR, mediante il quale si implementa il principio di responsabilizzazione ("accountability") e si dimostra in concreto come l'Ente intende concretamente adeguarsi al GDPR.

Per fare questo si deve prendere il documento

GDPR Scuole – DOC 003 – Reg Adeguamento GDPR Ver 1-0

farlo proprio inserendo i riferimenti dell'Ente ed approvarlo con Decreto del Dirigente Scolastico.

Passo 8: Approvare ed adottare le Disposizioni Operative per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione

Il riutilizzo e lo smaltimento non corretto di PC e di supporti di memorizzazione sono spesso la causa di violazioni di sicurezza, consistenti nella perdita di riservatezza di dati personali. Per questo motivo è necessario seguire adeguate procedure per la cancellazione in sicurezza dei dati.

A tale scopo si deve prendere il documento

GDPR Scuole – DOC004 – Reg Riutilizzo Smaltimento PC Ver 1-0

farlo proprio inserendo i dati dell'Ente ed approvarlo con Decreto del Dirigente Scolastico.

Passo 9: Effettuare una ricognizione dei trattamenti di dati affidati all'esterno

L'art. 28 del GDPR impone che con tutti i soggetti esterni che trattano dati personali per conto dell'Ente deve essere stipulato un vero e proprio contratto di "responsabile del trattamento dei dati". Per fare questo bisogna innanzitutto effettuare una ricognizione dei trattamenti di dati affidati all'esterno, compilando il modello

GDPR Scuole – DOC006 – Ricognizione Trattamenti Esterni.

Passo 10: Stipulare contratti di Responsabile del trattamento dei dati con i soggetti esterni

Per fare questo bisogna prendere il modello DOC006 di cui al punto precedente, e per ciascun soggetto esterno individuato, predisporre un apposito

contratto di "Responsabile del trattamento dei dati", personalizzando il modello standard predisposto nel file

GDPR Scuole – DOC010 – Contratto Responsabile Trattamento Dati Ver 3-0

e facendolo firmare a ciascun fornitore per accettazione.

Passo 11: Fornire le informative ai dipendenti ed ai cittadini

Il GDPR impone che le informative debbano essere essenziali, concise e sintetiche. A tal fine è stata predisposta una informativa per i dipendenti, contenuta nel file

GDPR Scuole – DOC007 – Informativa Dipendenti

ed un'informativa per i cittadini, contenuta nel file

GDPR Scuole – DOC008 - Informativa Genitori e Alunni

La prima , quella relativa ai dipendenti, può essere distribuita in formato cartaceo ai dipendenti assieme al cedolino paga, in duplice copia, di cui la copia firmata dal dipendente o collaboratore viene trattenuta a cura del datore di lavoro.

La seconda, quella relativa ai cittadini, deve essere pubblicata sul sito web dell'Ente all'interno della sezione "Privacy"; tutti i moduli, sia elettronici che cartacei, utilizzati dai cittadini per richiedere servizi all'Ente, devono contenere un rimando all'informativa pubblicata su sito web.

Passo 12: Attivare il processo di monitoraggio della sicurezza

La sicurezza non è una cosa statica, ma un condizione che può essere continuamente compromessa dal verificarsi di vari eventi, che devono essere oggetto di monitoraggio costante.

A tale scopo si utilizza il documento

GDPR Scuole – DOC009 – MMS

che deve essere compilato con frequenza settimanale da parte dell'Ente e successivamente inviato all'indirizzo MMS@datasecurity.it.

Passo 13: Effettuare un censimento degli account di administrator

Dal punto di vista della sicurezza, è estremamente importante tenere traccia degli account di administrator, e dei soggetti (persone fisiche) che materialmente accedono ai vari sistema con profilo di administrator o equivalente.

Per fare questo si deve compilare il modello

GDPR Scuole – DOC011 – Inventario Account di Administrator

e inviarlo alla mail dpo@datasecurity.it.

Passo 14: Effettuare una ricognizione del sistema informativo

E' importante avere sempre uno schema aggiornato del sistema informativo dell'Ente, o almeno un inventario dei componenti chiave che lo costituiscono.

Per fare questo si deve compilare il modello

GDPR Scuole – DOC012 – Ricognizione Sistema Informativo – Fase 1

e inviarlo alla mail dpo@datasecurity.it.