VADEMECUM

Regolamento EU 679/2016 GDPR

PER IL DIRIGENTE SCOLASTICO

Procedure da attuare a cura del Titolare del trattamento delle Istituzioni Scolastiche per la applicazione della normativa vigente in materia di tutela dei dati personali (Regolamento EU 679/2016 GDPR).

Sommario

Introduzione

LO SCOPO DI QUESTO VADEMECUM

Nell'ambito del Regolamento EU 679/2016 GDPR un ruolo fondamentale in materia di attuazione delle normative, di vigilanza e di attuazione delle misure minime di sicurezza previste spetta al Titolare del trattamento, ruolo che nella scuola è incarnato dal Dirigente Scolastico.

Crediamo di svolgere nel modo migliore il nostro compito di consulenti in materia rammentando al Dirigente quali sono i suoi obblighi e fornendo un agile manualetto per metterlo in condizioni di attuarli con naturalezza e senza troppa fatica.

Proprio queste esigenze di informazione e di affiancamento trovano risposta all'interno del presente manualetto destinato al Dirigente Scolastico; rivestendo il ruolo di Responsabile della Protezione dei Dati personali (D.P.O.) ci è sembrato fondamentale stilare un elenco di utili suggerimenti di natura tecnica, che tuttavia non si possono mai sostituire alle politiche organizzative e di miglioramento che solamente egli può (e deve) decidere, promuovere ed attuare.

LA STRUTTURA DEL VADEMECUM

Prefiggendosi uno scopo informativo, la presente guida vuole essere un "piccolo manuale" di facile e rapido uso e per questo tratta ogni argomento in modo diretto, "arrivando dritto al sodo", chiarendo in maniera schematica CHI (il soggetto obbligato), COSA (le azioni da intraprendere), e QUANDO.

SCANSIONE TEMPORALE

Il contratto con il quale il Dirigente Scolastico designa il Responsabile della protezione dei dati (D.P.O.) normalmente ha durata annuale. Questo vademecum propone una scansione degli eventi immaginando il trascorrere dell'Anno Scolastico e quindi da Settembre a Giugno, suggerendo le azioni migliori da intraprendere periodo per periodo.

Il contratto stipulato con Easyteam.org SRL

EasyGDPR

In questo capitolo troverà un riassunto schematico delle prestazioni incluse nel contratto stipulato con il Suo Istituto e denominato "EasyGDPR".

E' opportuno segnalare che le prestazioni elencate nel seguito si riferiscono ad un contratto "standard", cioè come previsto da Easyteam.org SRL e non modificato da richieste particolari che siano state avanzate dalla scuola in sede di capitolato di gara o richiesta di offerta.

L'ACQUISIZIONE DELL'INCARICO DI D.P.O.

La prestazione principale richiesta a Easyteam.org SRL e nominalmente a Ferdinando Bassi, è relativa all'acquisizione, da parte di quest'ultimo, dell'incarico di Data Protection Officer o di Responsabile della Protezione dei Dati (esterno) dell'Istituto Scolastico. L'incarico di R.P.D./D.P.O è regolamentato dall'Art. 39 del G.D.P.R. (Regolamento Europeo 2016/679), che ne descrive compiti, obblighi e responsabilità.

GLI ADEMPIMENTI BUROCRATICI

Il contratto prevede che Easyteam.org SRL si occupi degli adempimenti connessi alla designazione del D.P.O., che elenchiamo nel seguito del capitolo.

IL SOPRALLUOGO INIZIALE

Con la dicitura "sopralluogo iniziale" definiamo la presa visione di tutta la documentazione in possesso dell'Istituto ed elaborata in questi anni in merito a Codice della Privacy (D.Lgs 196/2003), Manuale di gestione del Protocollo Informatico, circolare AgID 2/2017.

I SOPRALLUOGHI PERIODICI

Il "sopralluogo periodico" prevede la verifica una volta all'anno della continuità della sussistenza delle misure minime di sicurezza previste dalla normativa, necessarie per il funzionamento degli uffici. Le misure di natura informatica saranno richieste all'Amministratore di Sistema designato dall'Istituto.

FORMAZIONE

L'Art. 29 del Regolamento EU 679/2016 recita:" Il *responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali* ***non può trattare tali dati*** *se non è istruito in tal senso dal titolare del trattamento…*".

Tale norma impone una vera e propria opera di formazione di tutto il personale in servizio. La nostra esperienza ci porta a suggerire di organizzare 2 tipologie di corso:

- Corso per Dirigente Scolastico e membri dello staff di Dirigenza, DSGA, Assistenti Amministrativi e funzioni strumentali che abbiano accesso a dati sensibili e/o giudiziari;
- Corso per tutti i Docenti ed i Collaboratori Scolastici.

La formazione così suddivisa, che si svolgerà interamente online, renderà possibile fornire nozioni affini ai trattamenti svolti.

DOCUMENTI

Dopo aver acquisito tutte le informazioni necessarie mediante i sopralluoghi iniziali e periodici e la ricezione di una tabella debitamente compilata dall'Istituto, Easyteam.org SRL sarà in grado di redigere/aggiornare i seguenti documenti:

- Documento delle misure a tutela dei dati delle persone
- Registro delle attività di trattamento (Art. 30 Regolamento UE)
- Valutazione d'impatto sulla protezione dei dati (D.P.I.A.) (Art. 35 Regolamento UE)
- Libro delle procedure
- Piano di attuazione
- Regolamento per l'uso di Internet e della Posta Elettronica (Provvedimento Garante 10/03/2007)
- Lettere di nomina dei Responsabili del trattamento e degli Incaricati del trattamento
- Informative (Artt. 13-15 Regolamento UE)
- Informativa per gli allievi
- Informativa per il personale
- Informativa per i fornitori
- Informativa per gli specialisti, tirocinanti, stagisti e studenti in alternanza
- Informativa generale per il sito istituzionale scolastico
- Informative personalizzate per i progetti

Incombenze del Dirigente Scolastico

VERIFICA DELLA VALIDITA' DELLA NOMINA DEL D.P.O.

L'Art. 37 comma 1 lettera a) del Regolamento UE 2016/679 prevede che la Autorità e gli organismi pubblici designino obbligatoriamente il D.P.O. e diano comunicazione di tale designazione all'Autorità Garante per la protezione dei dati personali mediante l'inserimento del nominativo e dei contatti del D.P.O. sul sito dell'Autorità stessa (attraverso procedura telematica).

All'inizio dell'anno scolastico è necessario verificare la sussistenza del rapporto contrattuale con la persona incaricata e rammentare che i dati di contatto della stessa, oltre che essere stati comunicati al Garante, siano pubblicati:

- Sul sito istituzionale della scuola (organigramma);
- Sulla intranet della scuola (area riservata del sito) o, in mancanza, affissi in bacheca;
- Citati in tutte le informative privacy redatte ai sensi degli Artt. 13-15 del Regolamento UE.

I dati da riportare sono i seguenti:

Il ruolo di D.P.O./R.P.D. per questo Istituto è svolto da:

Easyteam.org S.r.l. nella persona di Ferdinando Bassi – Via Walter Tobagi 2 – 20067 Tribiano (MI)

Contatto: rpd@easyteam.org Tel. 02-39430109

PREDISPOSIZIONE/AGGIORNAMENTO DI TUTTE LE INFORMATIVE PRIVACY

All'inizio di un nuovo Anno Scolastico è essenziale che tutto il nuovo personale venga regolarizzato sotto il profilo della privacy mediante consegna delle informative specifiche.

E' opportuno poi collocare, all'esterno dei locali di segreteria, del locale server e degli archivi, un cartello di divieto di accesso ai non autorizzati.

PREDISPOSIZIONE DELLE LETTERE DI NOMINA

All'inizio di un nuovo Anno Scolastico Easyteam.org SRL trasmetterà la RICHIESTA DI AGGIORNAMENTO DEI DATI sugli incaricati del trattamento. Questo ci consentirà la predisposizione delle lettere di nomina aggiornate.

ATTUAZIONE/MANTENIMENTO DELLE MISURE MINIME DI SICUREZZA PREVISTE

Una volta all'anno Easyteam.org SRL provvederà a verificare la sussistenza delle misure idonee di sicurezza previste per la tutela e la protezione dei dati.

Le misure idonee di sicurezza informatica sono predisposte dall'Amministratore di Sistema dell'Istituto Scolastico e la loro certificazione deve avvenire annualmente, per iscritto, da parte dello stesso.

A titolo non esaustivo si ricordano:

- La segreteria e la sala docenti devono essere luoghi ad accesso limitato e controllato (sportello, etc.);
- Gli armadi ed i cassetti che contengono dati personali devono essere chiusi a chiave;
- L'accesso ai dati (fascicoli) deve avvenire in modo differenziato in funzione dei miei "poteri";
- Ogni apparecchiatura che permette l'accesso alla rete deve essere protetta da password o altro sistema di autenticazione;
- Le credenziali di accesso devono essere complesse, personali e segrete;
- Le password devono essere cambiate ogni 3 mesi (segreteria) o 6 mesi (didattica);
- Il server deve concedere l'accesso esclusivamente ai dati di pertinenza dell'utente che accede;
- La rete deve essere protetta da sistemi anti-intrusione (**firewall**) e anti-distruzione (**antivirus**);
- Il back-up dei dati deve essere svolto almeno settimanalmente su supporti collocati in luoghi fisici diversi da quelli in cui risiedono gli originali;
- Il back up dei dati deve prevedere una **copia in luogo geograficamente diverso** (Cloud), di cui deve essere dimostrabile la sicurezza e l'aderenza al Regolamento EU 679/2016 GDPR
- Il back-up deve riguardare tutti i dati (lettere di word, schemi di excel) e non solo gli archivi principali (Argo, Axios etc.);
- Un file contenente la **descrizione delle misure idonee di sicurezza** informatica attuate a scuola, avente data certa (marca temporale) e firmato digitalmente dal Dirigente Scolastico, deve essere **tenuto a disposizione** per la sua comunicazione al Garante entro 72h in caso di violazione del sistema informatico (Circolare 2/2017 dell'Agenzia per l'Italia Digitale – AG.I.D.).

Incombenze del Direttore dei Servizi Generali Amministrativi

CONSEGNA DELLE LETTERE DI NOMINA AL PERSONALE AMMINISTRATIVO

Il Direttore dei Servizi Generali e Amministrativi (D.S.G.A.), in quanto capo della segreteria, svolge un ruolo importante ai fini dell'applicazione della normativa sulla Privacy a scuola che deriva dal fatto che la segreteria è, per definizione, il luogo in cui i dati vengono trattati in via principale.

All'inizio di un nuovo Anno Scolastico Easyteam.org SRL trasmetterà la RICHIESTA DI AGGIORNAMENTO DEI DATI sugli incaricati del trattamento. Questo ci consentirà la predisposizione delle lettere di nomina aggiornate.

VERIFICA DELLO STATO DI FORMAZIONE DEL PERSONALE AMMINISTRATIVO

Al Direttore dei Servizi Generali e Amministrativi spetta la verifica dello stato di formazione del personale amministrativo al fine, in caso di esito negativo, di organizzare quanto prima un corso stante quanto previsto dall'Art. 29 del Regolamento U.E. che recita: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento…*"

FORMAZIONE DI BASE DEI COLLABORATORI SCOLASTICI

Considerando il fatto che anche il personale collaboratore può trovarsi a trattare dati personali (indirizzi, informazioni inerenti allo stato di salute di allievi che necessitino di somministrazione farmaci o altro, attività di supporto alla segreteria etc.) è necessario che il corso più volte citato di cui all'Art. 29 del Regolamento U.E. venga svolto anche da questi ultimi.

VERIFICA DELLA CORRETTA GESTIONE DELLE INFORMATIVE

Il Regolamento UE 2016/679 agli Artt. 13-15 prevede che tutte le informative debbano essere semplici, chiare e comprensibili. Inoltre devono chiarire in modo dettagliato e specifico in cosa consiste il trattamento che si intende attuare.

Incombenze dell'Amministratore di Sistema

OBBLIGO DI ESEGUIRE UNA PROVA DI DISASTER RECOVERY

La normativa impone al Dirigente Scolastico, in qualità di Titolare del trattamento, di garantire, qualora un guasto, un attacco informatico o un virus dovesse distruggere i dati personali custoditi in formato digitale nei propri server, il loro completo ripristino grazie al perfetto funzionamento del sistema di backup entro 1 settimana dal momento dell'evento.

E' previsto che una simulazione di "Disaster Recovery" venga eseguita ogni anno.

OBBLIGO DI AGGIORNARE IL FILE DELLA DESCRIZIONE DELLE MISURE IDONEE DI SICUREZZA INFORMATICA IMPLEMENTATE

La Circolare 2/2017 dell'Agenzia per l'Italia Digitale (AG.I.D.) prevede che un file

- Redatto dall'Amministratore di Sistema
- firmato digitalmente dal Dirigente Scolastico;
- avente data certa (apposizione di marca temporale al file);
- contenente la dettagliata descrizione delle misure minime di sicurezza informatica implementate

sia redatto al fine di consultazione da parte dell'Autorità Garante per la protezione dei dati personali in caso di violazione, a vario titolo, del sistema informatico della scuola (data breach).

Tale file deve essere sempre tenuto aggiornato in caso di innovazione, modifica o riduzione delle misure idonee di sicurezza.

Gli Artt. 33 e 34 del Regolamento UE prevedono che, entro 72 ore da un episodio di violazione del sistema informatico ("data breach") sia data notifica al Garante e ai diretti interessati.

Contatti

Easyteam.org SRL

Via Walter Tobagi, 2 – 20067 Tribiano (Mi)

Tel: 02 39 43 01 09 - Fax: 02 45 50 34 67

www.easyteam.org

info@easyteam.org

easyteam@easypec.org

R.P.D. / D.P.O.

Ferdinando Bassi
Cellulare: 333.234.55.52

Email: rpd@easyteam.org

PEC: easyteam@easypec.org