Avv. Ernesto Belisario

LA PRIVACY A SCUOLA AI TEMPI DEL COVID-19

e-lex
STUDIO LEGALE

www.e-lex.it


© MARK ANDERSON
WWW.ANDERTOONS.COM
"Before I write my name on the board, I'll need to know how you're planning to use that data."

SOMMARIO

- La normativa vigente in materia di protezione dei dati personali: i princìpi applicabili
- I principali adempimenti privacy per le scuole: cosa cambia nelle attività a distanza
- Smart working e didattica a distanza: come scegliere la piattaforma
- Responsabilità e sanzioni

I - LA NORMATIVA VIGENTE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: I PRINCIPI APPLICABILI

GENERAL DATA PROTECTION REGULATION

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

Sommario

I Atti legislativi

REGOLAMENTI

* **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)** (1) 1

DECRETO LEGISLATIVO n. 101/2018

SERIE GENERALE

Anno 159° - Numero 219

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Mercoledì, 19 settembre 2018

AVVISO ALLE AMMINISTRAZIONI

SOMMARIO

DECRETO DEL PRESIDENTE DELLA REPUBBLICA
10 agosto 2018.

Ministero dello sviluppo economico

DECRETO 1 maggio 2018

DECRETO 5 agosto 2018

DATO PERSONALE

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

Art. 4, par. 1, GDPR

CATEGORIE PARTICOLARI DI DATI PERSONALI

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.

Art. 9, par. 1, GDPR

DATI RELATIVI A CONDANNE PENALI E REATI

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Art. 10, par. 1, GDPR

TRATTAMENTO

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.

Art. 4, par. 1, GDPR

PRINCIPI APPLICABILI AL TRATTAMENTO

I dati personali sono

- ☑ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
- ☑ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (limitazione della finalità);
- ☑ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);

PRINCIPI APPLICABILI AL TRATTAMENTO

I dati personali sono

- ☑ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- ☑ esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
- ☑ trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

PRINCIPIO DI ACCOUNTABILITY

Il titolare del trattamento è competente per il rispetto dei principi previsti dal GDPR e in grado di comprovarlo (c.d principio di «responsabilizzazione»).

(Art. 5, par. 2, GDPR)

PRIVACY BY DESIGN

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Art. 25, par. 1 GDPR

PRIVACY BY DEFAULT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Art. 25, par. 2 GDPR

ADEMPIMENTI PER LA SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a)la pseudonimizzazione e la cifratura dei dati personali;

b)la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c)la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d)una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

(Art. 32, par. 1, GDPR)

MISURE DI SICUREZZA

- Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

- Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento.

II - I PRINCIPALI ADEMPIMENTI PRIVACY PER LE SCUOLE: COSA CAMBIA CON LA DIDATTICA A DISTANZA

ADEMPIMENTI ORGANIZZATIVI

- ☑ Adeguamento dell'organizzazione della scuola al GDPR (definizione dell'ufficio competente per adempimenti, predisposizione istruzioni agli uffici e ai soggetti autorizzati);
- ☑ Individuazione e nomina del DPO;
- ☑ Adeguamento delle nomine dei responsabili esterni.

RESPONSABILE PROTEZIONE DATI

DPO INTERNO

- Nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

- Necessario apposito atto di designazione

DPO ESTERNO

- Nel caso dei DPO esterno, le funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica. Se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel GDPR.

- Necessario fare attenzione alla procedura di evidenza per la scelta del DPO (valore affidamento, requisiti partecipanti, SLA contratto)

GESTIONE IN FORMA ASSOCIATA

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

(Art. 37, par. 3, GDPR)

RESPONSABILE DEL TRATTAMENTO

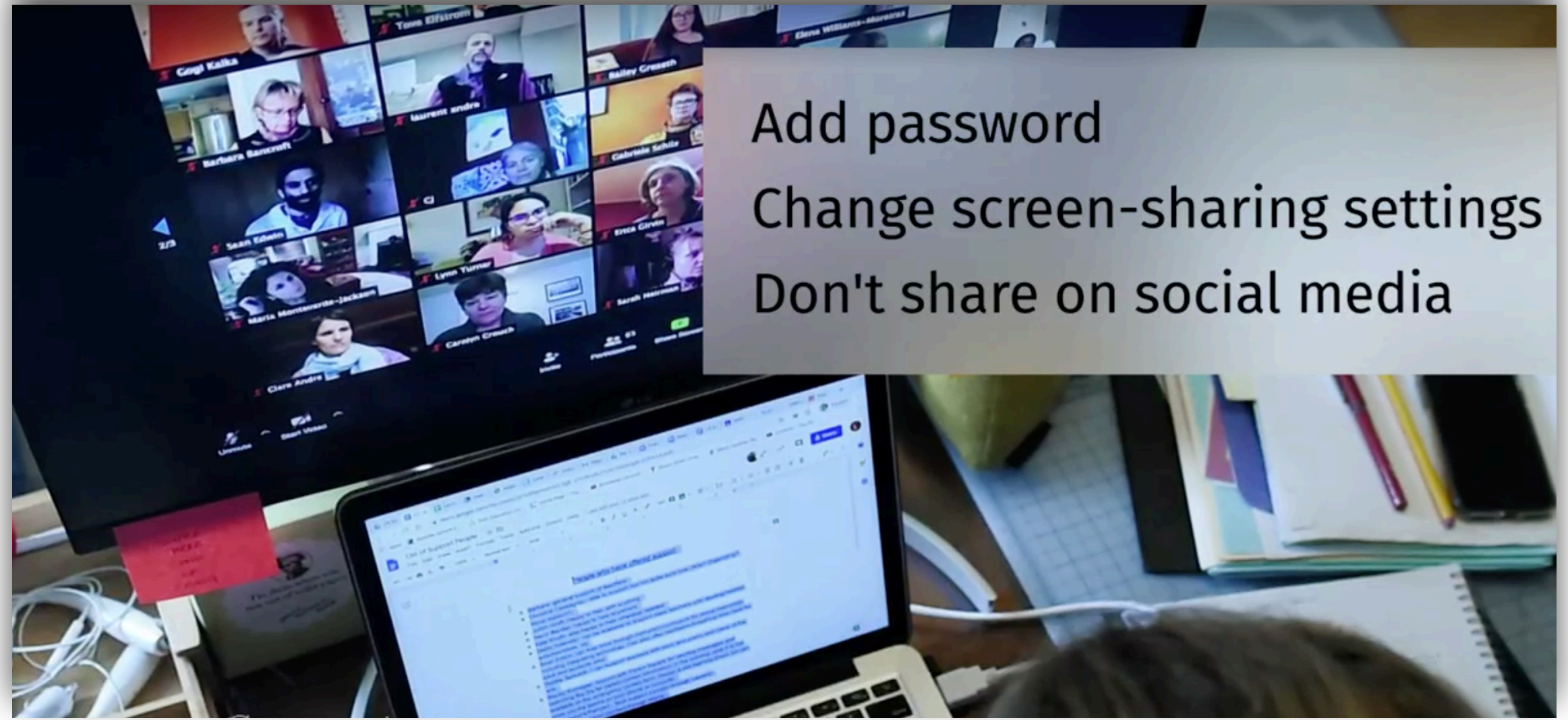
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Art. 4, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

- *trattare i dati personali soltanto su istruzione documentata del titolare del trattamento;*
- *garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*
- *adottare le misure di sicurezza;*
- *rispettare i limiti previsti per la nomina dei sub-responsabili;*
- *assistere il titolare del trattamento in relazione all'esercizio dei diritti degli interessati;*
- *cancellare o restituire al titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;*
- *mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.*

Art. 28, par. 3, GDPR


Add password
Change screen-sharing settings
Don't share on social media

DIRITTI DEGLI INTERESSATI

- Revisione e integrazione delle informative;
- Revisione modalità con cui gli interessati esprimono il consenso.

TRASPARENZA

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.
Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Art. 12, par. 1, GDPR

LA "NUOVA" INFORMATIVA

- Rispetto all'art. 13 del Codice Privacy, si prevedono numerose informazioni aggiuntive da fornire agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

- L'Informativa va resa per iscritto o con altri mezzi, anche elettronici.

- Anche oralmente, purché sia richiesto dall'interessato e sia comprovata con altri mezzi l'identità dell'interessato.

- Le informazioni possono essere fornite anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

LA "NUOVA" INFORMATIVA

Rispetto agli elementi obbligatori da indicare nell'informativa privacy ai sensi dell'art. 13 del Codice Privacy, i Titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni a:

- i dati di contatto del DPO;
- la base giuridica del trattamento a corredo della illustrazione delle finalità del trattamento;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il diritto di proporre reclamo al Garante per la protezione dei dati personali.


(N)EVER(S)TOP
LEARNING

QUALI ADEMPIMENTI PER LA DIDATTICA A DISTANZA?

Il Garante ha precisato che:

- non è necessario richiedere un nuovo consenso al trattamento, in quanto lo stesso è già stato validamente prestato attraverso l'iscrizione;

- qualora la scuola non abbia già provveduto, è necessario rilasciare/ integrare l'informativa ai sensi degli artt. 13 e 14 GDPR.

QUALI ADEMPIMENTI?

Il Garante ha precisato che:

Per garantire la **trasparenza** *e la* **correttezza** *del trattamento, le istituzioni scolastiche e universitarie devono* **informare** *gli interessati (alunni, studenti, genitori e docenti), con un* **linguaggio comprensibile** *anche ai minori, riguardo, in particolare, alle caratteristiche essenziali del trattamento che viene effettuato. Relativamente ai docenti, scuole e università, nel rispetto della disciplina sui controlli a distanza, dovranno trattare solo i dati strettamente necessari e comunque senza effettuare indagini sulla sfera privata.*

VALUTAZIONE D'IMPATTO

Le scuole dovranno effettuare una Valutazione degli impatti privacy (*Privacy Impact Assessment* – PIA) fin dal momento della progettazione del singolo procedimento e della scelta degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

(Art. 35 GDPR)

DIDATTICA A DISTANZA E VALUTAZIONE D'IMPATTO

Il Garante con la nota del 30 marzo 2020, ha specificato che:

"Non è necessaria la valutazione di impatto [..] se il trattamento dei dati effettuato dalle istituzioni scolastiche e universitarie, per quanto relativo a minorenni e a lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti".

REGISTRO DEI TRATTAMENTI

Ogni titolare del trattamento tiene un registro elettronico in cui sono riportate le seguenti informazioni:

a)il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b)le finalità del trattamento;

c)una descrizione delle categorie di interessati e delle categorie di dati personali;

d)le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e)ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

f)ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g)ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

(Art. 30, par. 1, GDPR)

Gestione dati obbligatori alunni	Gestione del percorso scolastico, formativo e amministrativo dell'alunno, anche in sede di contezioso; aggiornamento dell'Anagrafe Nazionale degli Studenti; aggiornamento dell'Anagrafe Provinciale degli Studenti	Utilizzo di servizi ICT; Utilizzo di strumenti di office automation; Gestione manuale	Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi e a scopo di inclusione degli alunni con DSA; adempimento degli obblighi previsti dal D.M. 692/2017	Raccolta; Registrazione; Conservazione; Estrazione; Consultazione; Elaborazione; Modifica; Comunicazione; Limitazione.	Esecuzione di un compito di interesse pub pubblici poteri del titolare derivante da nor nazionale
Gestione dati facoltativi alunni	Gestione del percorso scolastico, formativo e amministrativo dell'alunno	Utilizzo di servizi ICT; Utilizzo di strumenti di office automation; Gestione manuale	Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi previsti dal PTOF di istituto, attività extracurriculari e partecipazione a singoli progetti svolti dall'Istituto	Raccolta; Registrazione; Conservazione; Estrazione; Consultazione; Elaborazione; Modifica; Comunicazione; Limitazione; Cancellazione (limitatamente a quanto satbilito dalla legge); Distruzione (limitatamente a quanto stabilito dalla legge)	Consenso dell'interessato; Esecuzione d contratto con l'interessato o esecuzion misure precontrattuali adottate su richiest stesso;
Gestione contratto a tempo indeterminato - Personale docente	Gestione delle informazioni funzionali al perfezionamento dell'assunzione e alla gestione del rapporto di lavoro del personale docente a tempo indeterminato ;	Utilizzo di servizi ICT; Utilizzo di strumenti di office automation; Gestione manuale	Gestione degli aspetti relativi al trattamento giuridico ed economico del personale anche in sede contenziosa e disciplinare; verifica del possesso dei requisiti per l'assunzione,	Raccolta; Registrazione; Conservazione; Estrazione; Consultazione; Elaborazione; Modifica; Comunicazione; Limitazione	Esecuzione di un compito di interesse pub pubblici poteri del titolare derivante da nor nazionale; esecuzione di un contratt

CONSERVAZIONE E AGGIORNAMENTO DEL REGISTRO

Il registro deve essere mantenuto costantemente aggiornato per rispecchiare in maniera effettiva i trattamenti posti in essere dal titolare o dal responsabile.
Qualsiasi cambiamento riferito alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.
Il registro può essere cartaceo o elettronico, e deve recare la data di creazione e successivamente, le date degli aggiornamenti effettuati.

FIRMA GRAFOMETRICA

FIRMA GRAFOMETRICA

L'adozione della firma grafometrica richiede, da parte dell'istituto:

- ☑ L'identificazione certa dell'utente tramite documento di identità, l'informazione dello stesso circa i termini e le condizioni di utilizzo del servizio e la sua accettazione dei predetti termini e condizioni;
- ☑ La conservazione della copia del documento di identità e dell'accettazione, per almeno 20 anni;
- ☑ Specificazione delle caratteristiche del sistema e pubblicazione sul sito internet dell'istituto;
- ☑ Obbligo di informativa sul trattamento dei dati personali;
- ☑ Verifica delle garanzie e dell'affidabilità del fornitore.

III - SMART WORKING E DIDATTICA A DISTANZA: COME SCEGLIERE LA PIATTAFORMA

LAVORO AGILE E PRIVACY

"Il lavoro agile (o smart working) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività".

Art. 18, Legge n. 81/2017

LAVORO AGILE E PRIVACY

Il Governo, per la gestione dell'emergenza Covid-19, ha incentivato il ricorso a modalità di lavoro agile:

- Art. 2, comma 1, lett. r), DPCM 8 marzo 2020;
- Art. 4, comma 1, lett. a), DPCM 1 marzo 2020;
- Circolare 1/2020, Ministero per la Pubblica Amministrazione;
- Art. 87, Decreto Legge n. 18/2020 (CuraItalia).

LAVORO AGILE E PRIVACY

Raccomandazioni per i lavoratori

- Rispetto dei regolamenti interni sull'accesso e l'utilizzo delle risorse informatiche, della navigazione in Internet, della gestione della posta elettronica e dei documenti analogici;
- Adozione di particolari cautele qualora i lavoratori utilizzino dispositivi personali;
- Preferenza per l'utilizzo degli archivi in cloud;
- Particolare attenzione nella distruzione della documentazione cartacea;
- Comunicazione tempestiva di incidenti da cui potrebbe scaturire un data breach.

DIDATTICA A DISTANZA

L'attuale situazione di emergenza sanitaria ha determinato la sospensione dei servizi di educazione per l'infanzia e la chiusura di Scuole, Università e degli altri Istituti di formazione, facendo salva la possibilità di ricorrere allo svolgimento di attività formative a distanza.

COSA SI INTENDE PER DIDATTICA A DISTANZA?

"Il collegamento diretto o indiretto, immediato o differito, attraverso videoconferenze, videolezioni, chat di gruppo; la trasmissione ragionata di materiali didattici, attraverso il caricamento degli stessi su piattaforme digitali e l'impiego dei registri di classe in tutte le loro funzioni di comunicazione e di supporto alla didattica, con successiva rielaborazione e discussione operata direttamente o indirettamente con il docente, l'interazione su sistemi e app interattive educative propriamente digitali: tutto ciò è didattica a distanza".

Nota del Ministero dell'Istruzione del 17 marzo 2020

LE INDICAZIONI DEL GARANTE

- *Privilegiare soluzioni che abbiano sia dalla fase di progettazione e per impostazioni predefinite misure a protezione dei dati. Non è necessaria la valutazione di impatto qualora il trattamento dei dati effettuato dalle istituzioni scolastiche ed universitarie non presenti ulteriori caratteristiche suscettibili di aggravarne i rischi.*

Provvedimento Garante per la protezione dati personali 26 marzo 2020 n. 64

QUALI ADEMPIMENTI?

Il Garante ha precisato che:

- non è necessario richiedere un nuovo consenso al trattamento;
- qualora la scuola non abbia già provveduto, è necessario rilasciare l'informativa ai sensi degli artt. 13 e 14 GDPR;
- il trattamento deve essere improntato ai principi di cui agli artt. 5-6 GDPR;
- deve essere evitata qualsiasi forma di profilazione, comunicazione e diffusione dei dati raccolti;
- è necessario adottare adeguate misure di sicurezza tecniche e organizzative.

QUALI ADEMPIMENTI?

<u>Il Garante ha precisato che è necessario, per le scuole, procedere</u>:

- *"a stipulare contratti o atti di individuazione del responsabile del trattamento ai sensi dell'articolo 28 del Regolamento, che per conto delle stesse tratta i dati personali necessari per l'attivazione della modalità didattica a distanza".*

RICAPITOLANDO, QUALI CRITERI SEGUIRE PER LA SCELTA DEGLI STRUMENTI DA ADOTTARE PER LA DIDATTICA A DISTANZA?

1. Conformità ai princìpi di privacy by design e privacy by default;
2. Presenza di adeguate misure di sicurezza;
3. Per le Piattaforme che offrono servizi complessi deve essere presente la possibilità di effettuare una configurazione rispettosa del principio di minimizzazione.

IV- RESPONSABILITÀ E SANZIONI

IL SISTEMA SANZIONATORIO

Il GDPR definisce un impianto sanzionatorio molto più rigido di quello previsto dal Codice Privacy:

- ☑ €10.000.000 e fino al 2% del fatturato mondiale annuo;
- ☑ € 20.000.000 e fino al 4% del fatturato mondiale annuo;
- ☑ Responsabilità civile nei confronti dell'interessato che subisca un danno materiale o immateriale causato da una violazione del GDPR;
- ☑ Sanzioni penali (artt. 167-171 Codice Privacy).

COME SI STANNO COMPORTANDO I GARANTI EUROPEI?

SANZIONI IRROGATE

- Italia al primo posto con oltre 30 provvedimenti irrogati per un totale di 39.452.000 euro;
- Regno Unito (ICO) quale autorità più severa che ha irrogato un numero inferiore di sanzioni ma di importo molto elevato (la più elevata supera i 204 milioni di sterline);

Le infrazioni più spesso sanzionate:
-Trattamento illecito di dati;
-Insufficienti misure di sicurezza.

FACCIAMO QUALCHE ESEMPIO

CARENTI MISURE DI SICUREZZA

ICO sanziona per 320,000.00 € un'azienda operante in ambito farmaceutico per aver immagazzinato cinquecentomila documenti contenenti dati comuni e sanitari in contenitori non chiusi e lasciati nel retro di uno stabile; la società non ha protetto accuratamente i dati neppure dagli eventi atmosferici e l'acqua li ha distrutti.

SMARRIMENTO DI DISPOSITIVI

L'autorità spagnola ha sanzionato una società per lo smarrimento di 6 chiavette usb non cifrate che contenevano circa 11 mila dati personali.

I dispositivi esterni non possono essere utilizzati se non sono cifrati in quanto la perdita di tali dispositivi è un elemento fisiologico.

In caso di smarrimento inoltre, è necessario avvisare immediatamente il vertice aziendale.

VIOLAZIONE DEI PRINCIPI APPLICABILI AL TRATTAMENTO

Il Garante italiano ha sanzionato tre istituti (uno di Torino e due della Provincia di Napoli), con delle sanzioni di 4.000 euro, per aver illecitamente pubblicato i dati (sanitari e non) di numerosi docenti all'interno delle graduatorie presenti sui siti degli istituti.

CARENTI MISURE DI SICUREZZA

Il Garante italiano ha sanzionato la Provincia di Trento per aver inviato una mail, senza utilizzare il campo "copia nascosta", ai genitori di 16 bambini non in regola con l'obbligo di vaccinazione. Il Garante ha specificato che tale informazione rientra tra i dati relativi allo stato di salute.

La sanzione è stata limitata all'ammonimento, tenuto conto che è stata la stessa Provincia a segnalare la disattenzione da parte del dipendente.

CARENTI MISURE DI SICUREZZA

L'autorità rumena ha sanzionato una società per un utilizzo improprio di Whatsapp, che era usato dai dipendenti per finalità lavorative e per scambiarsi i dati dei clienti. L'utilizzo di tale applicazione comportava una modalità di trattamento dei dati non sicura che ha portato ad una sanzione di 150.000 euro.

CARENTI MISURE DI SICUREZZA

L'autorità norvegese ha comminato una sanzione di oltre 200.000 euro al dipartimento municipale per l'educazione di Oslo in quanto una scuola della città aveva distribuito un'app a genitori e studenti per dialogare con il personale scolastico. L'app aveva adeguate misure di sicurezza in quanto anche soggetti estranei all'istituto avevano la possibilità di avere accesso ai dati scolastici e alle informazioni personali degli alunni.

VIOLAZIONE DEI PRINCIPI DEL GDPR E CARENTI MISURE DI SICUREZZA

Il Garante italiano ha sanzionato l'Università La Sapienza per aver reso disponibili online le identità di due whistleblower a causa di inadeguate misure di sicurezza e controllo della gestione del sistema di whistleblowing, che non sono state in grado di limitare l'accesso a tali dati ai soli soggetti autorizzati. La sanzione di 32.000 euro è stata inflitta per violazione degli artt. 5 e 32 del Regolamento.

VIOLAZIONE DEL PRINCiPIO DI LICEITA' DEL TRATTAMENTO

L'Autorità spagnola ha comminato una sanzione di 3.000 euro a una scuola che aveva trasferito, senza alcuna base giuridica, delle foto di studenti a soggetti terzi che poi le hanno pubblicate.

CARENTI MISURE DI SICUREZZA

L'Autorità norvegese ha sanzionato, per oltre 73.000 euro, un comune che aveva i dati di 15 studenti minorenni, affetti da disturbi fisici e psichici, attraverso una piattaforma che non era stata sottoposta a DPIA. Inoltre, la piattaforma, non disponeva di adeguate misure di sicurezza e controllo degli accessi, tanto che, altri studenti, potevano accedere liberamente ai dati degli altri.

VIOLAZIONE DEL PRINCIPIO DI LICEITà DEL TRATTAMENTO

L'Autorità polacca ha sanzionato una scuola che aveva adottato degli scanner biometrici per il rilevamento delle impronte digitali degli alunni per il procedimento di pagamento della mensa. Il consenso fornito dai genitori non è stato ritenuto valido in quanto obbligatorio.

CARENTI MISURE DI SICUREZZA

L'Autorità islandese ha sanzionato una scuola (9.000 euro) in quanto un docente ha inviato via mail agli studenti e ai genitori un allegato contenente il rendimento scolastico degli alunni, senza adottare adeguate misure di sicurezza a protezione dei dati.

RESPONSABILITA' ERARIALE

Il pagamento della sanzione irrogata dal Garante della Privacy costituisce danno erariale.

(Corte Conti, Sezione giurisdizionale per il Lazio, Sentenza 28 maggio 2019, n. 246)

GRAZIE PER L'ATTENZIONE

www.e-lex.it
ebelisario@e-lex.it

e-lex
STUDIO LEGALE