

PRIVACY

E

DIDATTICA A DISTANZA

UNA GUIDA PER LE SCUOLE

Versione 2.0



STUDIO LEGALE
ASSOCIATO

MASI BORSARI
GIRANI QUERCIOLI

LO STUDIO

Multidisciplinarietà, forte integrazione delle competenze, specializzazione.

Partnership consolidate con società e professionisti esterni, formazione costante dei giovani.

Dal 1997, questi sono i punti di forza dello Studio Legale Associato Masi Borsari Girani Quercioli che, grazie alla specializzazione e all'interazione dei quattro soci e dei collaboratori suddivisi in due sedi, è in grado di offrire consulenza legale e assistenza giudiziale nelle diverse discipline giuridiche.

A Bologna e Forlì, un modo nuovo e più efficiente di vivere la professione legale, per un servizio di qualità al Cliente.

INTRODUZIONE

L'emergenza Covid19 ha imposto la chiusura degli istituti scolastici e l'utilizzo dell'informatica per poter assicurare l'erogazione di servizi.

Le lezioni da casa comportano alcuni rischi e necessità di organizzazione.

La didattica a distanza consente di collegare quotidianamente docenti e studenti, secondo diverse modalità, a seconda dello strumento di videoconferenza prescelto. Inoltre, sono innumerevoli i servizi per condivisione di documenti, correzione dei compiti online, creazione di webinar.

Il lavoro agile (c.d. "smart working") è disciplinato dall'art. 18-24 L. 81/2017 e permette di effettuare la prestazione lavorativa sia presso i locali aziendali che all'esterno.

Dal punto di vista della protezione dei dati personali lo stato d'emergenza non comporta nessuna deroga alla corretta applicazione degli istituti: sia con riferimento all'organizzazione della didattica a distanza che allo smart working, è necessario valutare, fin dalla progettazione, come trattare i dati personali in modo lecito, corretto, trasparente, sicuro, e proporzionale alle finalità.

INTRODUZIONE

Il Garante per la protezione dei dati personali in data 30 Marzo 2020 ha pubblicato il documento "Didattica a distanza: prime indicazioni", che riporta alcune utili informazioni.

Il Garante privacy ha invitato le scuole ad adottare iniziative per aumentare la consapevolezza dell'utilizzo degli strumenti e per sensibilizzare le famiglie e i ragazzi.

Il Garante invita le scuole a porre attenzione nella scelta e nella regolamentazione degli strumenti più utili per la realizzazione della didattica a distanza, anche nell'ottica del principio di minimizzazione.

Ecco il testo del Provvedimento sulla Didattica a distanza:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9302778>

In questa seconda versione dell'Help Book "Privacy e didattica a distanza. Una guida per le scuole" sono stati richiamati alcuni passaggi del provvedimento del Garante privacy.

**DAL PUNTO DI VISTA DELLA
PROTEZIONE DEI DATI PERSONALI,
DIDATTICA A DISTANZA E SMART
WORKING PRESENTANO MOLTI
TEMI TRA LORO SPECULARI, CHE E'
OPPORTUNO ORGANIZZARE IN
MODO SISTEMATICO.**



**Di seguito non verranno affrontati
gli aspetti giuslavoristici dello
smart working, ma viene
segnalata l'esigenza di dare
istruzioni precise a chi lavora da
casa, ai fini privacy.**

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY

Organizzare didattica a distanza (DAD) secondo l'approccio privacy by default consente di prevenire e gestire una serie di problemi pratici fin dall'inizio.



Ecco alcuni spunti di riflessione...

Immagini e webcam



Creazione di account



Impedire il controllo a distanza dei lavoratori



Utilizzo degli account aziendali da parte degli studenti



Si possono registrare le lezioni?

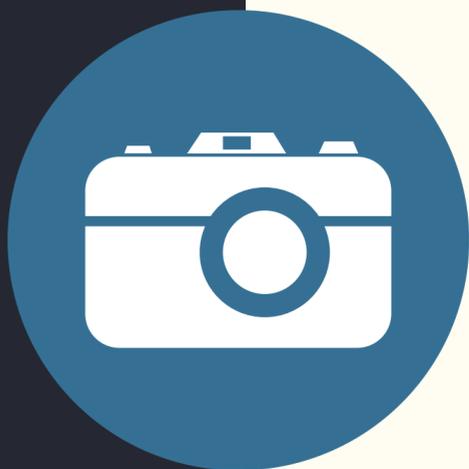


Dispositivi personali



DSA e BES

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Immagini e webcam

L'utilizzo della webcam ai fini della videoconferenza potrebbe non essere sempre necessario. I partecipanti dovrebbero essere in grado di autorizzare o meno il funzionamento della webcam per mostrare o meno la propria immagine.

Anche il docente è libero di mostrare o meno la propria immagine.

E' consigliabile dare indicazioni per salvaguardare il proprio contesto, come ad esempio suggerire impostazioni di sfocatura dello sfondo o invitare a prestare attenzione al contenuto del desktop in caso di condivisione dello schermo.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Creazione di account

La scuola dovrebbe scegliere se ricorrere a strumenti che richiedono o meno l'attivazione di account aziendali nominativi dei partecipanti oppure raccogliere account personali di studenti e docenti.

Ad esempio, nel caso in cui il docente avvii una videochiamata utilizzando Skype e invitando i singoli account personali di studenti o genitori, la scuola non ha controllo.

La creazione di una classe virtuale con strumenti dedicati (es. G Suite Classroom o Microsoft Teams) consente di poter accedere a impostazioni di sicurezza, regolare gli accessi, creare o disabilitare in ogni momento le classi virtuali.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Creazione di account

Secondo il Garante privacy, potrebbe essere sufficiente - per non dover designare ulteriori responsabili del trattamento - utilizzare servizi on line accessibili al pubblico e forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato.

Alcuni di questi servizi sono, peraltro, facilmente utilizzabili anche senza la necessaria creazione di un account da parte degli utenti.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Impedire il controllo a distanza dei lavoratori

La creazione di account o indirizzi di posta elettronica aziendali in capo ai lavoratori non autorizza il datore di lavoro ad accedere al contenuto in modo indiscriminato.

E' necessario adottare misure per la tutela dei lavoratori e regolare la fase di disattivazione degli account.

In particolare, il datore di lavoro dovrà limitarsi a utilizzare gli strumenti necessari, senza effettuare indagini sulla sfera privata o interferire con la libertà di insegnamento.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Utilizzo degli account aziendali da parte degli studenti

La creazione di account o indirizzi di posta elettronica aziendali in capo agli studenti dovrebbe essere regolato mediante misure tecniche che consentano di limitare alcune operazioni (es. Impedire l'invio e ricezione di messaggi al di fuori dell'organizzazione o del gruppo classe), coinvolgendo i genitori.

Se non sono previste o non è possibile adottare misure tecniche, si consiglia in ogni caso di stabilire, tramite regolamento, quali sono i comportamenti considerati leciti con gli account aziendali (es. Non è possibile iscriversi a TikTok utilizzando l'indirizzo email della scuola).

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Utilizzo degli account aziendali da parte degli studenti

Il trattamento di dati svolto dalle piattaforme per conto della scuola dovrà limitarsi a quanto strettamente necessario alla fornitura dei servizi richiesti ai fini della didattica on line e non per ulteriori finalità proprie del fornitore.

Ai dati personali dei minori, inoltre, va garantita una specifica protezione poiché i minori possono essere meno consapevoli dei rischi, delle conseguenze e dei loro diritti.



Si possono registrare le lezioni?

La scuola dovrebbe chiedersi se desidera registrare o meno le lezioni e se metterle a disposizione degli studenti, magari utilizzando uno storage cloud (es. OneDrive).

In tale caso, gli interessati dovrebbero essere informati di tale eventualità e dovrebbe essere precisato per quanto tempo verranno conservate le registrazioni.

Se i docenti o gli studenti intendono registrare il video per scopi personali è bene precisare che la scuola non ha responsabilità in caso di diffusione di registrazioni non autorizzate.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



Dispositivi personali

I docenti che utilizzano i propri dispositivi personali ai fini della prestazione lavorativa (c.d. "BYOD" Bring Your Own Device) devono garantire un adeguato livello di sicurezza, ad esempio utilizzando sistemi operativi e antivirus aggiornati, utilizzare reti e wifi sicuri, impostare credenziali di accesso, evitare la proliferazione di copie in locale.

Se il docente o il personale amministrativo utilizzano il dispositivo personale condividendolo con familiari (magari con i figli per utilizzo di social network o per guardare Netflix) è necessario consigliare ulteriori misure per evitare l'utilizzo promiscuo.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY



DSA e BES

Garantire l'applicazione dei piani educativi individuali tramite didattica a distanza è una sfida che richiede uno sforzo inedito.

Se alla videoconferenza partecipano studenti con bisogni speciali o disturbi di apprendimento specifico è necessario evitare ogni riferimento a tale situazione in presenza di altri partecipanti.

Prevedere modalità dedicate per assicurare l'applicazione degli strumenti compensativi e dispensativi. In caso di utilizzo di strumenti di storage cloud di documenti, è necessario regolare gli accessi per evitare comunicazioni illecite di dati particolari.

QUALI SONO I PUNTI DA APPROFONDIRE



Minimizzazione



Serve acquisire il consenso?



Sicurezza delle piattaforme



Contratto con le piattaforme



Trasferimenti dati extra UE



Minimizzazione

La scelta della piattaforma è essenziale.

In alcuni casi, potrebbe essere preferita una piattaforma di videoconferenza open source (come ad es. <https://jitsi.org/>) che, a differenza di servizi proprietari, non raccoglie e non conserva dati personali.

In questo modo l'organizzatore deve solo creare una stanza virtuale "usa e getta" e inviare il link di collegamento ai partecipanti.

Prima e dopo la call conference non è necessario, per l'organizzatore, trattare nessun dato personale o richiedere la creazione di account (ad es. Non è necessario tenere elenchi degli indirizzi o email da "aggiungere alla chiamata").

Questa modalità è consigliata per riunioni con il personale, con consulenti e fornitori, con i genitori.



Minimizzazione

In questi giorni è aumentata la curiosità per le varie piattaforme che consentono di effettuare videochiamate.

Si può cadere in errore, spesso di pensa che “se tutti le utilizzano allora saranno senz’altro lecite”.

La scuola, invece, deve conoscere lo strumento che utilizza, ciascuno ha proprie particolarità, e le impostazioni devono essere correttamente settate prima dell’utilizzo.

Ad esempio, la piattaforma Zoom (molto “in voga” in questo periodo) tra le sue impostazioni consente di controllare l’attenzione dei partecipanti e segnalarlo all’organizzatore o di generare un report (con un punteggio sul tempo di attenzione totale al meeting). Funzionalità come questa richiedono una valutazione di liceità da parte della scuola e l’adozione di misure tecniche e organizzative.



Minimizzazione

Si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti (evitando, ad esempio, il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità).

Minimizzare vuol dire anche ridurre gli oneri per le famiglie nel dover seguire i figli nelle operazioni necessarie per collegarsi alle aule virtuali.

Prevedere misure semplici aiuta le famiglie a organizzarsi tra didattica a distanza e lavoro agile.



Serve acquisire il consenso?

L'erogazione di servizi di didattica a distanza rientra nell'esecuzione del rapporto contrattuale e delle funzioni istituzionali, ma alcune funzionalità (es. Immagine tramite webcam) possono richiedere il consenso degli interessati.

Secondo il Garante privacy, non deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) uno specifico consenso al trattamento dei propri dati personali funzionali allo svolgimento dell'attività didattica a distanza.



Sicurezza delle piattaforme

Molti dei punti di attenzione finora suggeriti richiedono l'implementazione di misure tecniche, anche con riferimento alla sicurezza informatica.

E' pertanto necessario verificare se la piattaforma scelta garantisca standard sufficienti, o impostazioni di controllo in linea alle misure organizzative che si intende attuare.

La scelta di strumenti cloud adeguati è una valida alternativa all'utilizzo indiscriminato di dispositivi personali da parte dei docenti, offrendo ambienti sicuri dove salvare i dati o attraverso cui comunicare con gli studenti.



Contratto con le piattaforme

Le piattaforme di cui si avvale la scuola per la creazione di classi virtuali o per il salvataggio di documenti effettuano un trattamento di dati personali per conto della stessa, in qualità di responsabili del trattamento dei dati personali.

L'art. 28 GDPR richiede che tali soggetti sottoscrivano un contratto per garantire standard adeguati di sicurezza nei confronti del titolare del trattamento.

Le attività di didattica a distanza, talora fornite da alcuni registri elettronici, possono essere in alcuni casi già disciplinate nello stesso contratto di fornitura stipulato.



Trasferimento dati extra UE

Molte delle piattaforme di didattica a distanza o di smart working presenti sul mercato si basano su data center ubicati al di fuori dell'Unione Europea.

Ciò comporta che, sebbene i partecipanti a una videoconferenza o che condividono un documento su uno spazio cloud, si trovino su territorio italiano, i loro dati verranno salvati in un altro continente



Trasferimento dati extra UE

Il Regolamento Europeo n. 679/2016 impone al titolare di mappare tali situazioni nel proprio registro delle attività di trattamento ai sensi dell'art. 30

GDPR, individuare una base giuridica che renda lecito il trattamento (es. Verificando se il Paese di destinazione sia soggetto a una decisione di adeguatezza o se il fornitore del servizio abbia sottoscritto le clausole contrattuali standard della Commissione europea).

Gli interessati (studenti e docenti) devono essere informati in modo specifico sul trasferimento di dati che li riguardano.

QUALI SONO I RISCHI E I PROBLEMI IN CASO DI ASSENZA DI REGOLE?

Violazione di dati personali (Data Breach)

Qualora il titolare del trattamento non abbia implementato le misure finora descritte, o altre rese necessarie dal contesto, potrebbe verificarsi una violazione di dati personali, ad esempio potrebbe essere diffusa sulla rete internet un documento riservato o soggetti non autorizzati potrebbero accedere ai dati. In tali casi, potrebbe essere necessario "autodenunciarsi" entro 72 ore al Garante per la protezione dei dati personali.

L'utilizzo promiscuo di dispositivi personali utilizzati da parte di docenti o studenti è una possibile fonte di rischi di comunicazioni diffusione di dati illeciti.

Business continuity

L'organizzazione corretta di smart working e didattica a distanza limita le possibilità di interruzioni dei servizi a causa di eventi sopravvenuti.

Richieste di cancellazione e consenso

Gli interessati conservano la possibilità, in ogni momento, di revocare il consenso sul trattamento della loro immagine. Tale circostanza può essere impattante in caso di mancata regolazione di eventuali registrazioni.

COSA BISOGNA FARE

Il MIUR con nota del 17 Marzo 2020 ha invitato le scuole a prevedere una vera e propria “progettazione delle attività”, che veda il coinvolgimento del corpo docenti, del Dirigente Scolastico, dell’Animatore Digitale e del Team digitale.

Oltre alle questioni finora viste, altre misure suggerite dalla nota MIUR (come l’invio di video o di messaggi vocali) devono prevedere una progettazione anche a livello privacy. Ad esempio, nell’ambito della messaggistica istantanea (es. Whatsapp, Telegram) è preferibile l’utilizzo di canali piuttosto che di gruppi. La progettazione deve essere, quindi, globale in tutti gli ambiti.

La nota MIUR, inoltre, prescrive alle scuole statali precise istruzioni dal punto di vista della privacy, ovvero di informare gli interessati ai sensi degli articoli 13-14 GDPR, di stipulare contratti ex art. 28 GDPR per l’attivazione delle piattaforme di didattica a distanza, di garantire l’applicazione dei principi di cui all’art. 5 GDPR e di effettuare una valutazione di impatto sulla protezione dei dati personali di cui all’art. 35 GDPR.

Le misure indicate dal MIUR sono consigliabili a tutte le scuole e, inoltre, è necessario adottare misure organizzative che consentano di diffondere rapidamente, tra studenti docenti e famiglie, le regole per l’utilizzo corretto della didattica a distanza.

COSA BISOGNA FARE

Il Garante per la protezione dei dati personali in data 30 Marzo 2020 ha diffuso il proprio provvedimento "Didattica a distanza: prime indicazioni", nel quale precisa gli aspetti salienti inerenti la minimizzazione dei dati personali e limitazione delle finalità del trattamento, oltre a indicazioni sulla progettazione dei servizi di didattica a distanza.

In particolare, il Garante privacy restringe i casi in cui è obbligatorio effettuare una valutazione di impatto ex art. 35 GDPR.

Particolare attenzione è stata posta sulla scelta dei fornitori delle piattaforme e sulla trasparenza del trattamento.

COSA BISOGNA FARE

Effettuare una valutazione di impatto ex art 35 GDPR

La valutazione consente di seguire una metodologia per rilevare tutti i rischi e organizzare tutte le misure tecniche e organizzative.

Non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive.

ESEMPIO DI COME SI FA UNA DPIA:



<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

Aggiornare il registro delle attività di trattamento ex art. 30 GDPR

Il registro deve essere aggiornato con la descrizione dei nuovi trattamenti.

Informare gli interessati

Aggiornare o redigere nuove informative ai sensi degli art. 13-14 GDPR, con un linguaggio comprensibile anche ai minori in ordine, in particolare, alle caratteristiche essenziali del trattamento.

COSA BISOGNA FARE

Regolamento

Redigere un regolamento che definisca le misure che i lavoratori devono adottare per rendere sicuro il trattamento. Ad esempio, è necessario regolamentare l'utilizzo di dispositivi personali e utilizzo delle piattaforme. Tra le misure previste, attenzione particolare deve essere data all'aggiornamento dell'antivirus e del sistema operativo, dei rischi legati alla ricezione di email (c.d. Phishing), limitare l'uso della carta, limitare la conservazione di files su dispositivi personali, prescrivere l'utilizzo di wifi e reti sicure.

Vademecum e infografiche

Per creare una condivisione delle regole, è bene creare vademecum e infografiche che consentano a docenti e studenti di comprendere in modo veloce e efficace le misure da applicare. Ad esempio nel vademecum il docente potrebbe essere invitato, all'inizio della lezione, ad avvisare i partecipanti se la stessa verrà registrata, o visualizzare una slide con l'avviso in attesa dell'inizio della lezione. I vademecum potrebbero contenere consigli pratici sull'utilizzo delle piattaforme utilizzate, ad esempio mostrando i passaggi per eseguire la sfocatura dello schermo.

ESEMPIO DI INFOGRAFICA:

6.) USA WIFI E RETI ADEGUATAMENTE PROTETTE

Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette. Se necessario, aumenta la sicurezza della password del tuo Wi-Fi di casa.



ESEMPIO DI ISTRUZIONI PRATICHE:

<https://support.skype.com/it/faq/FA34896/cos-e-la-sfocatura-dello-sfondo-in-skype>

PROTEGGERE I DATI PER AVERE CURA

**La protezione dei dati personali
vuol dire "avere cura" ed è parte
del rapporto educativo.**

CONTATTI

Via San Vitale 40/3/a

Bologna

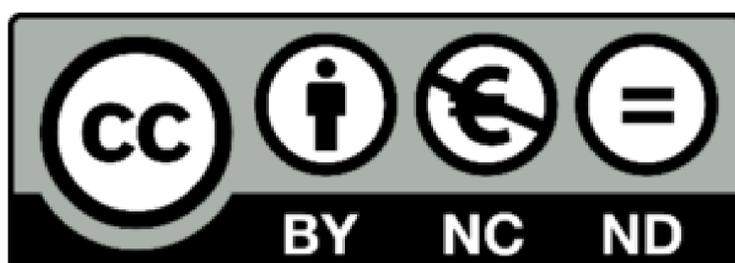
tel. 051.273730

www.studiolegaleassociato.biz



Avv. Elia Barbujani

ebarbujani@riparto.it



E' possibile condividere ogni contenuto per fini non commerciali citando l'autore, con divieto di elaborazione per ottenere opere derivate.

//

Un gruppo di liberi professionisti
uniti da uno scopo comune:
servire al meglio le persone
nei loro bisogni.

//



STUDIO LEGALE
ASSOCIATO

MASI BORSARI
GIRANI QUERCIOLO