Didattica Digitale Integrata:
adempimenti in materia di privacy

OXFirm Studio di Consulenza Contatti: tel. 06-87153238; Email: gdpr@educonsulting.it

partner Asso Edu

DIDATTICA DIGITALE INTEGRATA E TUTELA DELLA PRIVACY

Le istituzioni scolastiche per assicurare e procedere all'attività DID, devono porre in essere adeguati comportamenti a tutela della privacy.

Normativa di riferimento:

- Linee guida sulla DID , di cui al Decreto del Ministro dell'Istruzione del **26 giugno 2020, n. 39** (https://www.miur.gov.it/documents/20182/0/ALL.+A+_+Linee_Guida_DDI_.pdf/f0eeb0b4-bb7e-1d8e-4809-a359a8a7512f?t=1596813131027)

- Indicazioni operative in materia di protezione dei dati personali nella DID fornite in data **04.09.2020** da parte del Gruppo di lavoro congiunto Ministero dell'istruzione-Ufficio del Garante per la protezione dei dati personali. (https://www.istruzione.it/rientriamoascuola/allegati/Didattica-Digitale-Integrata-e-tutela-della-privacy-Indicazioni-generali.pdf)

- Indicazioni operative per lo svolgimento delle attività didattiche nelle scuole del territorio nazionale in materia di Didattica digitale integrata e di attuazione del decreto del Ministro della Pubblica Amministrazione 19 ottobre 2020. (https://www.miur.gov.it/documents/20182/0/m_pi.AOODPIT.REGISTRO+UFFICIALE%28U%29.0001934.26-10-2020.pdf/42f95694-4731-4f81-fd7f-ffa028cb5210?version=1.0&t=1603829435618)

Linee Guida sulla DID, Decreto del Ministro dell'Istruzione 26 giugno 2020 n.39

1. Forniscono indicazioni per la progettazione del **Piano scolastico per la didattica digitale integrata (DDI)** da adottare, nelle scuole secondarie di II grado, in modalità complementare alla didattica in presenza, nonché da parte di tutte le istituzioni scolastiche di qualsiasi grado, qualora emergessero necessità di contenimento del contagio, nonché qualora si rendesse necessario sospendere nuovamente le attività didattiche in presenza a causa delle condizioni epidemiologiche contingenti.

2. Il **Piano scolastico per la didattica digitale integrata (DDI)** deve individuare i criteri e le modalità per riprogettare l'attività didattica in DDI, a livello di istituzione scolastica, tenendo in considerazione le esigenze di tutti gli alunni e gli studenti, in particolar modo degli alunni più fragili.

Ulteriori Linee Guida del D. M. 26/07/2020 n.39

3. Il **Piano scolastico per la didattica digitale integrata (DDI)** va allegato o integrato nel Piano Triennale dell'Offerta Formativa.

4. Integrare il Regolamento d'Istituto con specifiche disposizioni in merito alle norme di comportamento da tenere durante i collegamenti da parte di tutte le componenti della comunità scolastica relativamente al rispetto dell'altro, alla condivisione di documenti e alla tutela dei dati personali e alle particolari categorie di dati (ex dati sensibili)

DIDATTICA DIGITALE INTEGRATA:
ADEMPIMENTI IN MATERIA DI PRIVACY

1. Individuazione degli strumenti digitali
2. Informativa privacy
3. Base giuridica del trattamento
4. Rapporto con il fornitore
5. Istruzioni operative per gli utenti
6. Misure di sicurezza tecniche ed organizzative

Account dedicato per piattaforme

- Compito della Scuola è individuare una **piattaforma che risponda ai necessari requisiti di sicurezza dei dati a garanzia della privacy** (cfr provvedimento Garante Privacy del 26 marzo 2020 e del 4 settembre 2020)

In conformità alle linee guida del Piano Nazionale per Scuola Digitale, la scuola può creare un dominio (@nomescuola.edu.it) - associato alla piattaforma G-Suite for Education.

Tanti sono i compiti delle Istituzioni scolastiche per adempiere agli obblighi dettati dalla normativa sulla privacy:

1. **Informativa:** le Istituzioni scolastiche , devono informare gli interessati in merito ai trattamenti dei dati personali effettuati nell'ambito dell'erogazione dell'offerta formativa. Occorre pertanto aggiornare l'informativa rilasciata agli interessati al momento dell'iscrizione o, nel caso del personale scolastico, al momento della stipula del contratto di lavoro, indicando gli eventuali nuovi fornitori del servizio che, in qualità di responsabili del trattamento, trattano i dati per conto dell'Istituzione stessa.

…Compiti della Scuola….

2. Deve informare, alunni e genitori, che riceveranno una casella di posta personalizzata con account cognomenome@nomescuola.edu.it. Ricordando che tale account permetterà l'accesso alla piattaforma; a non consentirne l'uso ad altre persone.
3. Occorre modificare la password iniziale fornita dall'Istituto al primo accesso; essendo l'account strettamente personale, conservare in sicurezza e mantenere segreta la password personale di accesso alla piattaforma e.learning.
La scuola deve altresì occuparsi della nomina del fornitore come **Responsabile esterno del trattamento dei dati** e della conservazione dei dati personali:
- In relazione a ciò , prevista dall'art.5, lettera e) del regolamento, è chiamata, (in persona di Titolare del Trattamento) ad assicurare che **i dati non siano conservati più a lungo del necessario;** disponendo che i dati siano cancellati al termine del progetto didattico.
- Laddove l'istituzione scolastica ritenga opportuno ricorrere a piattaforme più complesse che includono una più vasta gamma di servizi, anche non rivolti esclusivamente alla didattica, sarà necessario verificare, con il supporto del RPD, che siano **attivati solo i servizi strettamente correlati con la DDI** configurando i servizi 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).

Procedure da attivare/verificare per garantire la conformità al GDPR delle attività connesse alla DaD e DID

Si deve fare in modo che le applicazioni per la videoconferenza siano gestite in un ambiente riservato (ad esempio Meet tramite il dominio riservato G Suite), evitando applicazioni per la videoconferenza che mettono a disposizione stanze "pubbliche" per le attività. Tanto si rende necessario per garantire che i partecipanti alle attività siano solo ed esclusivamente gli aventi diritto ed evitare la presenza di utenze estranee e non autorizzate. In alternativa si rende necessario (laddove possibile) proteggere l'accesso al meeting tramite un codice riservato o altra procedura similare. In ogni caso, deve sempre essere possibile identificare la presenza di utenze esterne e non approvate, durante un meeting e più in generale durante qualunque attività riferita alla DaD e DID.

Procedure da attivare/verificare per garantire la conformità al GDPR delle attività connesse alla DaD

2) Attenzionare le procedure messe a disposizione dagli strumenti per la videoconferenza relative alla registrazione del meeting. Tale registrazione (sia da parte dei docenti che degli allievi) è da considerarsi legittima se utilizzata a scopi esclusivamente personali. È esclusa qualsiasi forma di diffusione o comunicazione senza il consenso esplicito di tutti gli interessati. Ovviamente, la responsabilità della comunicazione o della diffusione è direttamente relazionata al singolo individuo. Anche la disabilitazione (ove possibile) di tale funzione non risolve alla radice il problema: sarebbe, comunque, possibile e banalmente con altri strumenti registrare il meeting (così come sarebbe possibile durante l'attività in presenza). La soluzione è da ricercarsi nel livello di consapevolezza e responsabilità dell'utenza.

IN SINTESI…. MISURE TECNICHE

1. adozione di misure atte a garantire la disponibilità dei dati (es. **backup e disaster recovery**);
2. utilizzo di sistemi di protezione perimetrale, adeguatamente configurati in funzione del contesto operativo;
3. utilizzo di sistemi antivirus e anti malware costantemente aggiornati;
4. utilizzare sistemi operativi e applicativi supportati dai produttori e aggiornamento periodico dei software di base al fine di prevenirne la vulnerabilità;
5. registrazione degli accessi e delle operazioni compiute in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati;
6. definizione di istruzioni da fornire ai soggetti autorizzati al trattamento;
7. formazione e sensibilizzazione degli utenti.

Norme di comportamento per gli utenti (studenti)

- A comunicare immediatamente attraverso email all'Istituto l'impossibilità ad accedere al proprio account, il sospetto che altri possano accedervi, ed episodi come lo smarrimento o il furto della password;
- a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma di didattica a distanza;
- a non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- ad osservare le presenti norme di comportamento, pena la sospensione da parte dell'Istituto dell'account personale dello Studente e l'esclusione dalle attività di didattica a distanza e dai progetti correlati;
- ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della Scuola;
- a non diffondere in rete le attività realizzate dal docente, con il docente e i compagni;
- a non diffondere in rete screenshot, fotografie o filmati relative alle attività di didattica a distanza.

Norme di comportamento per gli utenti (studenti)

- custodire con cura e diligenza le credenziali per l'accesso ai servizi informatici, aggiornandole con frequenza (possibilmente ogni tre mesi), non divulgandole né cedendole a terzi per alcun motivo ed evitando di salvarle nel pc, utilizzando sistemi di memorizzazione automatica;
- assicurarsi di aver eseguito il logout da qualsiasi piattaforma web o dai programmi utilizzati al termine della sessione di lavoro;
- Divieto di condivisione delle credenziali di accesso con soggetti terzi e consentire l'accesso alla piattaforma a soggetti non autorizzati
- non salvare documenti contenenti dati personali sulla memoria del computer o su altri dispositivi elettronici. Al termine del lavoro, rimuovere e cancellare dalla memoria del computer o di altri dispositivi elettronici (videocamera, fotocamera ecc..) i dati personali eventualmente presenti;
se necessario, utilizzare servizi di cloud storage (Google Drive, Dropbox, Icloud, One Drive, ecc.) istituzionali o dispositivi di memoria rimovibili, ricorrendo sempre a sistemi di archiviazione sicuri (pseudonimizzare o cifrare i documenti).
Ricordare che lo spazio web eventualmente messo a disposizione dalla scuola deve essere utilizzato solo per fini didattici; è severamente vietato depositare materiale personale non pertinente all'attività didattica
- gli studenti devono entrare con puntualità nell'aula virtuale (quando necessario);
- rispettare le consegne del docente, partecipare ordinatamente ai lavori che vi si svolgono, presentarsi ed esprimersi in maniera consona ed adeguata all'ambiente di apprendimento;
- svolgere le attività a distanza proposte dai docenti sulla piattaforma didattica con puntualità e con cura.

Norme di comportamento per gli utenti (famiglie)

- Preparare i discenti o far preparare gli stessi, per tempo, alla lezione: sveglia in anticipo, creazione di un ambiente adatto e uno stile in linea con quanto gli alunni/studenti facevano a scuola. È il modo di dire loro che questa parte importante della loro quotidianità non è persa.
- Lasciare autonomia ai discenti nella relazione con l'insegnante ed i compagni: bisogna lasciar loro il proprio spazio senza togliere la libertà che hanno a scuola. L'ideale sarebbe, persino, lasciare usare loro le cuffie auricolari, e che il genitore cambi ambiente in casa, se possibile.
- Vigilare sull'uso delle applicazioni e/o della piattaforma: ogni tanto sbirciate e controllate unicamente il modo in cui stanno usando il dispositivo perché non si distraggano, ad esempio, con funzioni non utili.
- Si raccomanda di non interferire in quello spazio di libertà che caratterizza il rapporto educativo fra docente e alunno nel corso dei contatti giornalieri, di intervenire solo su richiesta dello stesso insegnante, se lo ritiene utile o necessario.

Norme di comportamento per gli utenti (famiglie)

Anche le famiglie devono adottare comportamenti corretti:

- Al termine di uno spazio-lezione si suggerisce ai genitori di non esprimere commenti o giudizi negativi davanti al proprio figlio/a (discente) su ciò che eventualmente si è sentito o visto. Questo per non interferire nella dinamica didattica e sulle relazioni docente-alunno e, quindi, per non minare l'autorevolezza della figura del docente.

- Controllare che svolgano i compiti assegnati, ma senza correggerli: l'errore è il più importante dispositivo di apprendimento. Non togliamolo ai ragazzi

- Eventuali osservazioni possono essere fatte direttamente ai docenti negli spazi e nelle modalità istituzionali note.

- Si ricorda ai genitori che, in base alla normativa vigente in materia di privacy e di cyberbullismo non è consentito alcun utilizzo non autorizzato di immagini, video-audio lezioni e materiale prodotto durante le attività di e.learning e teleconferenza. In particolare è fatto espressamente divieto di: filmare o registrare, catturare screenshot dei contenuti presenti nelle piattaforme senza autorizzazione del docente e condividerli in qualunque sede o canali social.

Norme di comportamento per gli utenti (docenti)

- Si ribadisce l'importanza e la necessità di un contatto giornaliero e costante nel tempo fra docenti e allievi. Oltre a raggiungere tutti gli alunni, è indispensabile assicurare tutti i giorni, degli spazi-lezione, con cadenza regolare fino al termine dell'anno scolastico. Con le indicazioni date in tema di organizzazione:

- i Consigli di classe, di interclasse e di intersezione stabiliscano un prospetto settimanale di video-lezioni "in diretta", da comunicare per tempo alle famiglie, cercando di mantenerlo stabile da una settimana all'altra, così da creare un ordine e un ritmo regolare nella giornata e nella settimana degli studenti e delle famiglie;

- organizzino alloro interno le modalità di erogazione delle lezioni sia attraverso la piattaforma e.learning sia attraverso teleconferenza

- privilegiare uno strumento o l'altro fermo restando l'obbligatorietà e l'uso di metodologie che rispecchino la nuova necessità di rendere la didattica vicina ai discenti

Norme di comportamento per gli utenti (docenti sostegno)

- Anche per i docenti di sostegno si ribadisce che occorre assicurare un contatto quotidiano con gli allievi DVA, partecipando almeno ad uno spazio-lezione giornaliero insieme ad un collega di disciplina e con tutto il gruppo classe, se possibile. Laddove è presente, si deve operare in stretta sinergia con l'educatore, che può partecipare allo spazio-lezione. Il contatto formativo con l'allievo DVA può essere pensato anche come attività didattica on line in piccolo gruppo. Nel caso non sia possibile neppure questa modalità di lavoro, il docente di sostegno assicurerà in ogni caso il contatto diretto giornaliero con l'allievo e la famiglia.

OBBLIGO GENERALE

Verifica e monitoraggio sul corretto trattamento dei dati personali nella DDI da parte di tutti (personale scolastico, famiglie, studenti) di questo processo, anche attraverso specifiche **iniziative di sensibilizzazione** atte a garantire la massima consapevolezza nell'utilizzo di strumenti tecnologici e nella tutela dei dati personali al fine di **evitare l'utilizzo improprio e la diffusione illecita dei dati personali trattati per mezzo delle piattaforme e il verificarsi di accessi non autorizzati e di azioni di disturbo durante lo svolgimento della didattica.** Ricordare a tutti i partecipanti, attraverso uno specifico "disclaimer", i **rischi che la diffusione delle immagini e, più in generale, delle lezioni può comportare, nonché le responsabilità di natura civile e penale.**

Doveri per i docenti

- Compilazione del registro elettronico;
- di tutta l'attività svolta il docente dovrà lasciare quotidianamente traccia su Registro elettronico. In particolare;
- occorrerà indicare le video lezioni svolte, l'argomento trattato, i lavori assegnati, le eventuali verificare che proposte.
- il registro elettronico è lo strumento ufficiale attraverso il quale il docente attesta il proprio lavoro giornaliero.
- nessun docente che risulta in servizio deve ritenersi esonerato da tale dovere.

Valutazione d'impatto

Particolare attenzione va rivolta alla configurazione dei **siti e delle App** messe a disposizione dell'istituzione scolastica per la fruizione dei materiali e per l'erogazione delle attività didattiche a distanza, nel rispetto del principio di privacy by design e by default previsto dal Regolamento. In particolare, nell'uso di tali strumenti, è necessario **evitare l'inserimento di tracker e analytics, notifiche push (per le App), font resi disponibili da terze parti, advertising o in-appurchasing,** o altri elementi che possono peraltro comportare il trasferimento di dati fuori dall'Unione Europea e/o il monitoraggio delle attività degli utenti.

Valutazione di impatto:

La valutazione di impatto deve essere effettuata solo SE e QUANDO ricorrono i presupposti dell'articolo 35 del Regolamento.

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 (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici). Essa va effettuata, nel caso di ricorso a piattaforme di gestione della didattica che offrono funzioni più avanzate e complesse che la scuola decida di utilizzare e che comportano un rischio elevato per i diritti e libertà delle persone fisiche.

Verifiche che la scuola deve effettuare

prima di procedere ad una valutazione d'impatto

1. rientra nei **casi previsti dall'art.35, par. 3 del Regolamento** (trattamento automatizzato, profilazione, trattamento su larga scala di categorie particolari di dati personali, ecc.),tenendo conto sempre del contesto in cui il trattamento stesso si colloca;

2. comporta la compresenza di almeno di due criteri individuati come indici sintomatici del **"rischio elevato"** dal Gruppo di lavoro ex articolo 29 delle Linee guida in materia di valutazione d'impatto sulla protezione dei dati (trattamenti valutativi o di scoring), compresa la ***PROFILAZIONE :*** **processo decisionale automatizzato, monitoraggio sistematico, dati sensibili o dati aventi carattere altamente personale, trattamento di dati su larga scala espressi in percentuale della popolazione di riferimento, creazione di corrispondenze o combinazione di insiemi di dati, dati relativi a interessati vulnerabili, uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, trattamento che in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".**

QUANDO E' LECITO IL TRASFERIMENTO DEI DATI PERSONALI TRANSFRONTALIERO DA PARTE DEL TITOLARE DEL TRATTAMENTO?
CASO SCHEREMS

A seguito delle rivelazioni di Edward Snowden sulla partecipazione di Facebook ed altri provider di servizi statunitensi al programma di sorveglianza di massa del governo USA denominato "PRISM", nel 2013, Maximillian Schrems, attivista austriaco, presentava denuncia al *Data Protection Commissioner* irlandese sostenendo l'illecito trattamento dei suoi dati personali che sarebbero stati trasferiti negli USA e sottoposti al controllo massivo delle autorità governative statunitensi, insieme a quelli di milioni di cittadini europei. Ciò sarebbe stato facilitato dall'accordo noto come "Safe Harbor", approvato nel 2000 dalla Commissione UE, che consentiva il libero trasferimento, a certe condizioni, dei dati personali tra UE e USA.Dopo aver deferito la questione alla Corte di giustizia dell'Unione europea, accoglieva le doglianze di Schrems con sentenza C-362/14 del 6 ottobre 2015 (sentenza "Schrems I"), invalidando la decisione 2000/520/CE con cui la Commissione UE aveva giudicato adeguato il livello di protezione [illegible] *Privacy Principles* e rinviando la questione al Garante irlandese per una nuova

Nel contempo: Privacy Shield

Nel frattempo, anche su invito del Gruppo di lavoro ex art. 29 (oggi "*European Data Protection Board*" o "EDPB") che raccoglie tutte le autorità privacy degli Stati Membri, a febbraio 2016, la Commissione EU e il Dipartimento del Commercio degli USA trovarono un accordo denominato «*Privacy Shield*»che avrebbe dovuto risolvere i problemi di inadeguatezza sollevati dalla Corte di Giustizia relativamente al *Safe Harbor*. Il *Privacy Shield*, approvato dalla Commissione UE con Decisione 2016/1250 del 16 luglio 2016, tra le altre cose, prevedeva obblighi più severi per le imprese statunitensi che importano dati personali di cittadini europei, un controllo periodico del rispetto di tali obblighi con conseguente applicazione di sanzioni e la previsione di garanzie e obblighi di trasparenza per l'accesso del governo e delle autorità pubbliche USA ai dati personali trasferiti per fini di contrasto e sicurezza nazionale.

Il Rinvio al Data Protection Commissioner irlandese

Anche a seguito dell'avvento del Regolamento (UE) n. 679/16 ("GDPR") – che ha sostituito la Direttiva 95/46/CE e tutte le normative locali di recepimento – era inevitabile che il giudizio di rinvio pendente innanzi al *Data Protection Commissioner* irlandese implicasse una nuova valutazione di adeguatezza della tutela prevista dal citato Privacy Shield e, più in generale, delle cd. "clausole contrattuali standard" ("SCCs"), anch'esse approvate dalla Commissione UE come valida misura di garanzia contrattuale per garantire la protezione dei dati personali dei cittadini UE in caso di trasferimento fuori dal territorio comunitario.Infatti, nel maggio 2018, l'High Court irlandese, investita del caso, deferiva alla Corte di Giustizia diverse questioni concernenti la validità dei trasferimenti effettuati con le SCCs e del Privacy Shield, ponendo l'accento sulla possibile violazione degli articoli 7, 8, 47 e 52 della Carta dei diritti fondamentali dell'UE.

Sentenza SCHREMS II: Corte di Giustizia Europea 16/07/2020

Con la sentenza del 16 luglio 2020 (sentenza “Schrems II”), la Corte di Giustizia ha dichiarato invalida la Decisione 2016/1250 con cui la Commissione UE aveva certificato l’adeguatezza della protezione dei dati personali offerta dal *Privacy Shield* per i trasferimenti tra UE e USA.In breve, secondo la Corte, la normativa interna degli USA in materia di accesso e di utilizzo, da parte delle autorità statunitensi, di dati trasferiti dall’UE non soddisfa i principi alla base del GDPR, tra cui quello di proporzionalità, in quanto esiste la possibilità da parte delle autorità pubbliche e di controllo degli USA di accedere e trattare i dati personali trasferiti senza limitazioni a quanto sia strettamente necessario per le ragioni di sorveglianza.In pratica, la carenza osservata dalla Corte si traduce in una mancanza di diritti effettivi degli interessati nei confronti delle autorità statunitensi. A tale riguardo, la Corte ha ritenuto, tra le altre cose, che il meccanismo del difensore civico (il cd. “*Ombudsperson*” ossia il “Mediatore dello Scudo”) previsto dal Privacy Shield non fornisce effettivamente garanzie equivalenti a quelle richieste dal diritto dell’UE, come ad esempio assicurare l’indipendenza del difensore civico e l’esistenza di norme che conferiscono al difensore civico il potere di adottare decisioni vincolanti per i servizi di intelligence e per le altre autorità pubbliche statunitensi.Al contrario, la sentenza non impatta direttamente sulla validità delle SCCs approvate dalla Commissione UE per il trasferimento di dati a Paesi extra-UE, sebbene la Corte abbia chiarito che, salvo il caso in cui esista una valida decisione di adeguatezza della legge privacy del Paese importatore dei dati adottata dalla Commissione UE, l’autorità di controllo di ciascuno Stato Membro è tenuta a sospendere o vietare un trasferimento di dati personali verso un Paese extra-UE quando ritenga, alla luce delle circostanze specifiche, che le SCCs non siano o non possano essere rispettate in tale Paese e che la protezione dei dati trasferiti, richiesta dal diritto dell’Unione, non possa essere garantita con altri mezzi.

Dal caso specifico si evince:

- **Trasferimento soggetto a garanzie adeguate.**

In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito **garanzie adeguate** e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (art. 46).

In particolare, il Titolare del trattamento potrà trasferire i dati personali **sulla base di accordi contrattuali, stipulati tra il titolare stabilito in Unione Europea e i soggetti destinatari dei dati stabiliti fuori dall'Unione Europea** (quali ad esempio responsabili esterni o contitolari del trattamento), che forniscano **garanzie adeguate** agli utenti (esempio l'esercizio da parte di questi dei diritti a loro accordati dal GDPR). Per **la conclusione di tali accordi contrattuali,** la Commissione Europea ha emanato dei **modelli standard.** L'esportatore dei dati deve incorporare tali clausole contrattuali in un contratto utilizzato per il trasferimento, così garantendo che i dati saranno trattati conformemente ai principi stabiliti nel regolamento europeo anche nel Paese terzo di destinazione. Anche queste decisioni della Commissione sono vincolanti per gli Stati dell'Unione.

GARANZIE ADEGUATE:

NON E' NECESSARIA L'AUTORIZZAZIONE DELL'AUTORITA' DI CONTROLLO

Possono costituire garanzie adeguate senza necessità di autorizzazioni specifiche da parte dell'Autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le **norme vincolanti d'impresa** in conformità dell'articolo 47;
c) le **clausole tipo** di protezione dei dati adottate dalla **Commissione** secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) le **clausole tipo** di protezione dei dati adottate da **un'autorità di controllo** e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un **codice di condotta** approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un **meccanismo di certificazione approvato** a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessa

NECESSARIA L'AUTORIZZAZIONE DELL'AUTORITA' DI CONTROLLO PER IL TRASFERIMENTO DEI DATI

a) **clausole contrattuali** tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o

b) **disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici** che comprendono diritti effettivi e azionabili per gli interessati.

LINK UTILI:

Sono stati messi a disposizione della scuola dei link utili per il trattamento dei dati nel contesto scolastico, riferiti proprio all'emergenza sanitaria:

FAQ GARANTE PRIVACY- Trattamento dati nel contesto scolastico nell'ambito dell'emergenza sanitaria

1. https://www.garanteprivacy.it/temi/coronavirus/faq#scuola
2. https://www.istruzione.it/coronavirus/didattica-a-distanza.html

indicazioni per il "tutoring": le scuole potranno mettersi in contatto, anche tramite la rete INDIRE, con scuole già esperte di didattica a distanza e che intendano mettersi a disposizione per socializzare le pratiche di utilizzo di ambienti di apprendimento virtuali;

LINK UTILI:

3. https://www.istruzione.it/coronavirus/didattica-a-distanza_inclusione-via-web.html: L'inclusione via web

Uno strumento pensato per affiancare e supportare il lavoro dei dirigenti scolastici, del personale e degli insegnanti nei percorsi didattici a distanza per gli alunni con disabilità.

All'interno delle pagine online sono messi a disposizione riferimenti normativi, condivisione di esperienze didattiche, link utili, *webinar*. Nel canale dedicato sono anche messe a disposizione, gratuitamente, piattaforme telematiche certificate per la didattica a distanza, grazie al contributi di privati che hanno risposto alla *call* lanciata dal Ministero dell'Istruzione. Il canale sarà costantemente aggiornato e arricchito di nuovi spunti e materiali.

4. https://innovazione.gov.it/coronavirus-solidarieta-digitale-in-tutta-italia/:

Sul portale messo a disposizione dal Ministero per **l'Innovazione tecnologia e la Digitalizzazione**, con il supporto tecnico dell'Agenzia per l'Italia Digitale, sono disponibili infatti offerte di giga gratuiti utili, fra l'altro, per facilitare la didattica a distanza.

SLIDE E MATERIALE ALLEGATO DELLA PRESENTAZIONE SARÀ INVIATO VIA EMAIL AI PARTECIPANTI

GRAZIE DELLA VS. ATTENZIONE

DOTT. CARMINE ARRICALE
PRIVACY@OXFIRM.IT