

Corso per lo sviluppo dell'alfabetizzazione ai Social Media nella scuola

Che cosa è il GDPR?

Cosa sono i dati personali?

Cosa si intende per elaborazione dati?

Chi deve attenersi alle norme del GDPR?

La normativa GDPR

Pubblicità basata sui comportamenti

Cosa fare in caso di infrazione

MODULO 6



Norme sulla protezione dei dati nel contesto dei Social Media – GDPR

Cofinanziato dal
programma Erasmus+
dell'Unione europea



Erasmus+ ref.no. 2019-1-R001-KA201-063996

Il sostegno della Commissione europea alla produzione di questa pubblicazione non costituisce un'approvazione del contenuto, che riflette esclusivamente il punto di vista degli autori, e la Commissione non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni ivi contenute.

Finalità del Modulo

Quando si ha a che fare con i Social Media, entrano inevitabilmente in gioco la privacy e la protezione dei dati.

Il mondo digitale di oggi ci permette di condividere tutto con tutti. Qualsiasi persona, organizzazione, azienda e persino governo elabora informazioni su di te, si occupa della tua scuola, del tuo comune o città, del tuo club sportivo, del tuo datore di lavoro ecc. Inoltre, la maggior parte delle informazioni su di te viene raccolta tramite Internet. Molte informazioni personali vengono condivise soprattutto attraverso siti social network, come Facebook e Instagram. Un malinteso comune è che i servizi delle piattaforme di Social Media siano gratuiti: in realtà si paga, ma invece che con i soldi, si paga con i dati personali.

Anche se i social possono essere un bel modo per interagire con gli amici e persino un mezzo divertente per fare nuove amicizie, la condivisione di informazioni personali comporta anche dei rischi. Tutto ciò che viene condiviso online può lasciare “impronte digitali”. Una volta che una foto, un video, uno stato, un tweet ecc. vengono pubblicati su Internet (ad es. sul proprio profilo dei social media), non se ne ha più il controllo: chiunque può copiare, ripubblicare o salvare la foto, rendendo impossibile cancellarla completamente da Internet. Queste impronte digitali possono essere "dati personali" (ad esempio il nome, l'indirizzo (e-mail), la data di nascita, le immagini). La condivisione di questo tipo di dati può esporre a ogni tipo di rischio (es. furto di identità, molestie, contenuti personalizzati, pubblicità mirata e molto altro). Pertanto, è importante sapere quali dati personali vengono raccolti, in che modo, per quanto tempo sono conservati e cosa si può fare per proteggere i dati personali. Ed è proprio qui che è intervenuto il legislatore.

I propri dati personali non possono essere semplicemente utilizzati da altri, né si possono utilizzare i dati personali di altre persone. Già da un po' di tempo esistono leggi sulla privacy che limitano l'uso dei dati personali. A causa dell'ascesa dei Social Media, di altre piattaforme online, delle applicazioni mobili, ecc., tutte basate sul trattamento di grandi quantità di dati personali, queste leggi sono diventate obsolete e non più in grado di fornire una protezione efficace per le persone e i loro dati personali. Pertanto, queste leggi nazionali sono state sostituite dal Regolamento Generale sulla Protezione dei Dati (GDPR), applicabile in tutta l'Unione Europea.



Il GDPR obbliga chiunque tratti dati personali al rispetto delle norme del regolamento, che riguarda anche scuole e insegnanti. Considerato che i bambini trascorrono una parte significativa del loro tempo sui Social Media e che le scuole sono importanti raccoglitori di dati personali (sul loro personale e sugli studenti sia online che offline), i temi trattati in questo modulo sono di grande importanza.

La privacy e la protezione dei dati sono diritti fondamentali per tutti. È importante che i giovani conoscano il GDPR e siano consapevoli dei loro diritti e doveri al riguardo. Gli insegnanti che spesso sono un primo punto di riferimento per gli studenti, sono in una posizione chiave per informare e sensibilizzare gli studenti sul GDPR.

Number of hours: 2

Obiettivi di apprendimento

- Rendere gli studenti e gli insegnanti consapevoli e familiari con il GDPR, le sue finalità e la sua importanza;
- Conoscere gli obblighi per le aziende e gli enti in materia di trattamento dei dati personali nel rispetto del GDPR;
- Conoscere i propri diritti riguardo al trattamento dei propri dati personali;
- Comprendere il concetto e il valore di “dati personali” e di “trattamento”;
- Creare un comportamento spontaneo negli studenti a riflettere prima di condividere i dati personali, nella consapevolezza che le informazioni che intendono condividere non siano troppo personali e non mettano a repentaglio la loro privacy;
- Sviluppare consapevolezza sulla normativa di protezione dei dati personali: cosa si può trovare o dovrebbe potersi trovare in una politica sulla privacy;
- Saper utilizzare le impostazioni sulla privacy della propria piattaforma di Social Media per garantire che solo le persone scelte possano accedere alle informazioni sul proprio profilo;
- Riconoscere la pubblicità mirata;





- Sapere, in qualità di istituzione scolastica e di insegnanti, come utilizzare legalmente i Social Media;
- Sapere cosa fare in caso di utilizzo illecito dei dati personali;

Materiali didattici

Contesto

1.1. Cosa è il GDPR?

Il Regolamento Generale sulla Protezione dei Dati è entrato in vigore il 25 maggio 2018 e si applica a qualsiasi organizzazione con sede nell'UE o al di fuori dell'UE, ma che elabora dati personali di persone dell'UE, comprese le scuole o qualsiasi altro istituto di istruzione. Attraverso l'introduzione di nuove regole, il GDPR mira a restituire alle persone il controllo sui propri dati personali limitando il modo in cui altre persone e organizzazioni possono utilizzare i dati personali.

Il GDPR protegge i dati personali dal momento in cui questi dati vengono condivisi con altri. Nessuno può semplicemente condividere, salvare, copiare, collegare... questi dati. Il GDPR stabilisce le regole che le aziende, gli enti e i governi devono seguire nel caso in cui desiderino avvalersi di dati personali di persone fisiche: il trattamento deve avvenire in modo lecito, corretto e trasparente. Inoltre, il GDPR stabilisce una serie di diritti per aiutare le persone a mantenere il controllo sui propri dati personali.

Poiché la condivisione di informazioni personali sui siti di social network o lo scambio di dati personali per l'accesso ad app e altri servizi basati sul Web è sempre più diffusa, questo modulo si concentrerà sul GDPR e sulla protezione dei dati alla luce di tali servizi.





1.2. Cosa sono i dati personali?

1.2.1. In generale

I dati personali consistono in qualsiasi tipo di informazione che riveli qualcosa di personale.

Per esempio, sono dati personali nome, codice fiscale, data di nascita, indirizzo, dati sulla posizione, foto o video di una persona, religione, indirizzo IP, cronologia di navigazione, marchi, schede comportamentali, profili sui Social Media (inclusi i *Mi piace*, condivisioni e amici) ecc.

Il significato di dato personale deve essere interpretato in modo molto ampio: tutte le informazioni che rendono possibile identificare una persona fisica direttamente o indirettamente sono da considerarsi come dati personali.

- Informazioni dirette:

Le informazioni che consentono di per sé di identificare la persona a cui si riferiscono .

Per esempio. nome, numero di telefono, codice fiscale, indirizzo di casa, indirizzo e-mail, dati sulla posizione, registrazioni vocali, ecc.

- Informazioni indirette:

Le informazioni che, in quanto tali, non sono sufficienti a identificare una persona, ma tenendo conto di informazioni aggiuntive – che sono già disponibili o che devono essere ottenute da un'altra fonte – consentono di identificare la persona interessata.

Per esempio: le targhe automobilistiche possono essere considerate dati personali, indipendentemente dal fatto che non si possa avere accesso diretto la database che collega le targhe ai proprietari di auto. Il fatto che altre persone possano effettuare questa connessione è sufficiente per qualificare queste informazioni come dati personali. Lo stesso ragionamento si applica alle informazioni raccolte da cookie, ID digitali e indirizzi MAC e IP (che sono univoci per ciascun dispositivo).

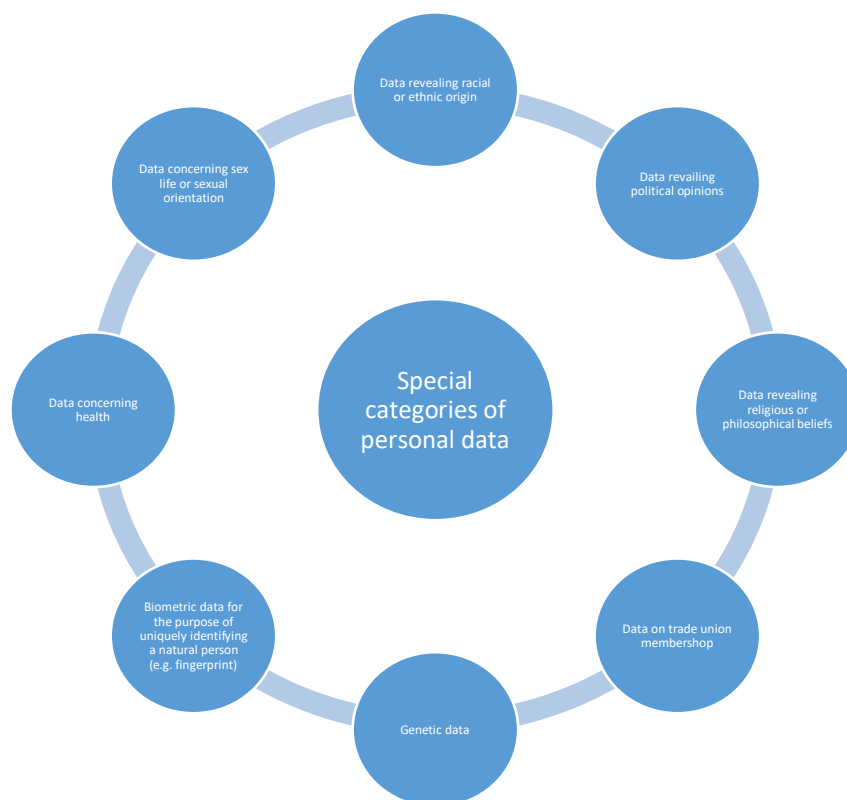
Una singola informazione (ad es. Il colore dei capelli, l'occupazione, la marca dell'auto...) potrebbe non essere in grado di identificare una persona fisica in quanto tale, ma può diventarlo quando questi dati vengono combinati con altri. Le aziende che raccolgono più tipi di dati sulle persone (es. Social Media) dovrebbero tenerne conto.



Dati personali
Informazioni relative a una <u>persona fisica</u> Non informazioni su aziende e altri enti, persone decedute, animali domestici, oggetti ecc.
Il <u>formato</u> è irrilevante: testo, immagine, video, suono ecc.
L'informazione che consente di identificare una sola persona, direttamente o indirettamente (tenendo conto di ulteriori informazioni)

1.2.2. Categorie speciali di dati personali

Il GDPR opera una distinzione tra dati personali "generali" e categorie speciali di dati. A causa della natura sensibile di questi ultimi e dell'ampio potenziale di incidere negativamente sulla privacy di qualcuno e su altri diritti e libertà fondamentali (ad esempio il diritto a non essere discriminati) durante l'utilizzo, in linea di principio, è vietato il trattamento di questo tipo di dati personali.



1.2.3. Perché i dati personali sono così preziosi?

I dati personali sono spesso chiamati “il petrolio di Internet”, la nuova valuta del mondo digitale di oggi. In altre parole, i dati personali sono considerati estremamente preziosi. Molte aziende offrono i loro servizi online gratuitamente, ma guadagnano dalla pubblicità. Si tratta di pubblicità che beneficia prevalentemente del trattamento dei dati personali.

In ambiente online si lasciano impronte digitali. Lo stato di avanzamento attuale della tecnologia consente alle aziende di utilizzare e archiviare i dati personali che si generano quando si acquistano determinati beni o servizi, o semplicemente quando si cercano determinati beni o informazioni (il nome, gli interessi, i desideri, lo stile ecc.). Un certo numero di clic e di *Mi piace* sui Social Media (ad es. Facebook) sono sufficienti per consentire alle aziende di condurre un'analisi per determinare le esatte preferenze di quella specifica persona. Combinando tutte le informazioni provenienti da diverse fonti, le aziende sono in grado di ottenere un'immagine chiara dell'utente. È qui che risulta evidente il valore dei dati personali: se un'azienda sa cosa si sta cercando o cosa interessa, è in grado di inviare annunci pubblicitari specifici per questi prodotti o servizi. (Ulteriori approfondimenti sul tema nel paragrafo 4. **Pubblicità mirata**)

I dati personali non interessano solo alle aziende, ma anche agli hacker! Negli ultimi anni, diverse grandi aziende sono finite sotto la luce della ribalta per gli scandali di hacking, come ad es. per furto dei dati personali dei propri clienti (es. Cambridge Analytica, Facebook, Mastercard).

Infine, i dati personali forniscono anche informazioni interessanti per le autorità pubbliche, in quanto possono consentire loro di acquisire nuove conoscenze su individui o gruppi di individui.

Un utilizzo incontrollato dei dati personali, tuttavia, potrebbe mettere in una posizione di potere aziende private, hacker e autorità pubbliche.

1.3. Cosa si intende per elaborazione dati?

Le regole del GDPR si applicano solo al trattamento dei dati personali.

Trattamento= Elaborazione, qualsiasi operazione o insieme di operazioni eseguite su dati personali o su insiemi di dati personali, anche con mezzi automatizzati.



Per esempio: raccogliere, registrare, organizzare (creare una mailing list), strutturare, archiviare, adattare o alterare, recuperare, consultare, utilizzare, divulgare tramite trasmissione, diffondere o mettere a disposizione in altro modo (pubblicare un messaggio o un'immagine sulla pagina Facebook di un'organizzazione), allineare o combinare, limitare, cancellare o distruggere i dati personali.

Se una delle suddette azioni viene svolta sui propri dati personali, si applica il GDPR.

È importante notare che il trattamento per attività puramente personali o domestiche non rientra nel GDPR. (ad es. genitori che scattano foto del loro bambino e dei compagni di scuola a un evento scolastico da tenere a casa in un album fotografico).

1.4. Chi deve attenersi alle norme del GDPR?

Il GDPR si applica a una società o ente (ossia persona fisica o giuridica, autorità pubblica, agenzia o altro organismo), indipendentemente dalle dimensioni, dal settore, dal numero di dipendenti o dal fatturato, che:

- tratta i dati personali nell'ambito delle attività di una delle sue filiali situate in UE (indipendentemente dal luogo in cui i dati vengono elaborati);
- è situato al di fuori dell'UE, ma tratta dati personali che emergono dall'offerta di beni/servizi a persone in UE o dal monitoraggio del comportamento di persone che si trovano in UE.

Tali società o enti sono considerati titolari del trattamento dei dati personali e devono garantire il rispetto del GDPR.





Le norme

2.1. I principi del GDPR

Qualsiasi azienda o ente che tratta dati personali dovrà seguire determinate regole.

2.1.1. Legittimità, correttezza e trasparenza

(a) Legittimità

Quando un'azienda o un'organizzazione desidera trattare i dati personali di un utente, prima di farlo, deve assicurarsi che il suo trattamento abbia una base giustificativa – una **base legale** – ai sensi del GDPR. Una base legale è una ragione del trattamento determinata e accettata dal GDPR (si veda l'articolo 6 del GDPR).

Le più rilevanti di queste basi legali che si riferiscono ai Social Media sono: per eseguire il trattamento dei dati personali è **necessario un contratto**, la società o l'organizzazione deve aver ottenuto il **consenso** dell'utente, oppure la società o l'organizzazione deve avere uno o più interessi legittimi nel trattamento dei dati personali dell'utente.

Necessità di un contratto

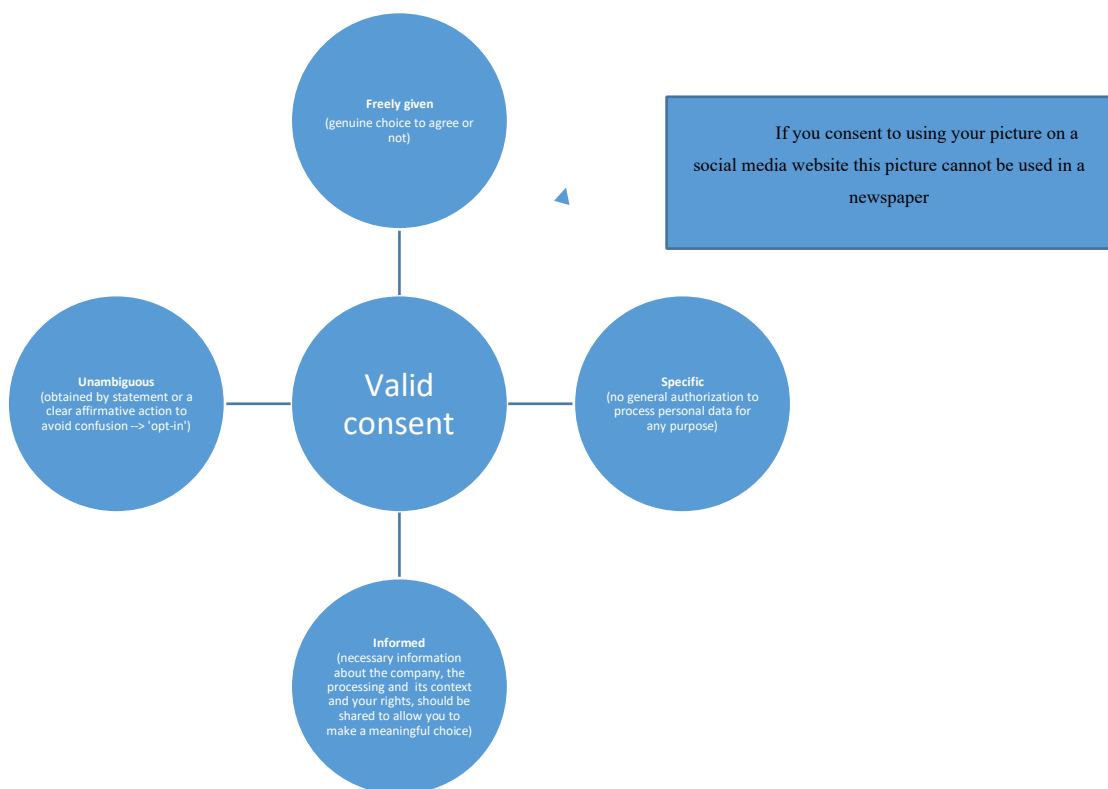
Quando un'azienda o un ente ha necessità di trattare dati personali per adempiere ad obblighi contrattuali che intercorrono con l'utente, o per eseguire richieste precontrattuali da parte dell'utente, può fare affidamento sulla base giuridica del “contratto”. Alcuni obblighi contrattuali semplicemente non possono essere adempiuti senza la raccolta e l'elaborazione di determinati dati personali. Non rientrano in questa base giuridica i trattamenti utili, ma non oggettivamente necessari, per l'esecuzione della prestazione contrattuale o per l'adozione di atti precontrattuali rilevanti.

Ad esempio: Twitter elabora i dati personali degli utenti, come nome e indirizzo e-mail, al fine di creare il loro account, di autenticare per consentire la creazione di contenuti.



Consenso

Il consenso ha un significato particolare nel GDPR. Per essere valido, il consenso deve rispondere a determinate caratteristiche:



Ciascun utente deve essere poter revocare il proprio consenso in qualsiasi momento. Le informazioni su come farlo devono essere fornite nel momento in cui viene chiesto di acconsentire a una determinata attività di trattamento. Il modo per revocare il consenso deve essere altrettanto semplice del darlo e non deve comportare conseguenze negative per l'utente (ad esempio una tariffa o livelli di servizio inferiori).

Ad esempio: Facebook ha una funzione di riconoscimento facciale che consente al sito del social network di riconoscere l'utente dalle foto o dai video sulla sua piattaforma. L'uso di tale funzionalità comporta il trattamento di dati personali, in particolare foto o video dell'utente. Per attivarlo, Facebook chiede il suo consenso.



Lo stesso vale per la funzione “Cronologia delle posizioni” offerta da Facebook. Quando si acconsente all'uso di questa funzione, i dati sulla posizione vengono elaborati al fine di esplorare ciò che accade intorno all'utente, mostrargli annunci pubblicitari pertinenti, cercare amici nella zona.

Ad esempio: Twitter elabora le informazioni raccolte dall'utente su Twitter, le altre sue attività online e i dati dei suoi partner al fine di mostrare pubblicità personalizzata all'interno e all'esterno di Twitter, in base al suo consenso.

Un'azienda o un'organizzazione può elaborare i dati personali di un bambino, fino a una certa età, solo con il consenso esplicito del genitore o tutore. La soglia di età per ottenere il consenso dei minori direttamente da loro può variare all'interno dei paesi dell'UE da 13 a 16 anni. (Questo aspetto può essere verificato con l'autorità nazionale per la protezione dei dati)

Interesse legittimo

Gli interessi legittimi per i quali è necessario il trattamento dei dati personali possono essere quelli dell'utente o gli interessi di terzi (ad es. interessi commerciali, interessi individuali o vantaggi sociali più ampi). Questo tipo di interesse deve essere specificato nell'informativa sulla privacy.

Per poter fare affidamento in maniera fondata su questo terreno di elaborazione, le aziende o le organizzazioni devono elaborare i dati degli utenti in un modo che sia ragionevolmente prevedibile, senza arrecare danni ingiustificati. In caso contrario, è probabile che gli interessi dell'utente prevalgano su quelli della società o dell'organizzazione, il che significa che non sono autorizzate a trattare i suoi dati personali (su questa base legale), a meno che non vi sia una giustificazione convincente per il trattamento.

Per esempio: Twitter estrapola deduzioni dagli account, come interessi, età e sesso dell'utente, al fine di fornire funzionalità come suggerimenti all'account, quali pubblicità, consigli, classifica della sequenza temporale ecc.

Per esempio: YouTube (Google) tratta i dati personali degli utenti per i loro legittimi interessi e quelli di terzi, applicando nel contempo adeguate garanzie a tutela della sua privacy. Questo è ad esempio il caso della personalizzazione dei propri servizi per fornire una migliore esperienza





all'utente, del marketing per informarli sui loro servizi, ma anche per fornire pubblicità, che mantiene gratuiti molti dei servizi stessi. (Quando gli annunci sono personalizzati, è richiesto il consenso)

Categorie speciali di dati

È importante aggiungere che per categorie particolari di dati personali sono previste 10 eccezioni al divieto generale di trattare tali dati (cfr. articolo 9 del GDPR). Se una di queste condizioni è soddisfatta, categorie particolari di dati possono essere legittimamente trattate. L'eccezione più importante alla luce dei Social Media è quando c'è il **consenso esplicito** della persona che è interessata ai dati personali.

Queste eccezioni costituiscono un ulteriore livello di condizioni oltre alle regole abituali. In pratica ciò significa che, quando si vogliono trattare categorie particolari di dati, è necessario che sussista un fondamento legittimo (art. 6) e deve essere applicabile un'eccezione (art. 9).

Per esempio: Google chiede il consenso prima di condividere le informazioni personali dei suoi utenti al di fuori dell'azienda. Supponiamo che un utente effettui una prenotazione di un ristorante tramite "Google Home", gli verrà chiesto il permesso prima di condividere i dati personali (es. nome, numero di telefono) con il ristorante. Quando si tratta di informazioni personali sensibili (es. allergie), si impegnano a chiedere il consenso esplicito.

(b) Equità

L'azienda o l'ente che tratta i dati personali dovrebbe farlo in modo equo, ovvero in modo che sia ragionevolmente prevedibile e in un modo che non causi effetti negativi ingiustificabili o che sia fuorviante.

(c) Trasparenza

Questo è un principio molto importante, legato all'equità! Fin dall'inizio, le aziende o le organizzazioni devono essere chiare, aperte e oneste con i propri utenti su come utilizzeranno i loro dati personali. Ciò richiede che le informazioni siano fornite in un linguaggio facilmente accessibile e comprensibile. È qui che entra in gioco la politica sulla privacy. Le politiche sulla privacy lunghe e complicate dovrebbero essere evitate secondo il GDPR.



L'informativa sulla privacy

L'informativa sulla privacy contiene tutte le informazioni su come i propri dati personali vengono raccolti, utilizzati e protetti dai Social Media (o qualsiasi altro sito Web). Ogni politica sulla privacy deve contenere un gran numero di elementi obbligatori:

- nome e recapiti della società/organizzazione
- dati di contatto del responsabile della protezione dei dati, se ne ha uno
- le finalità del trattamento dei dati personali e su quali basi legali elaborano i dati
- il legittimo interesse al trattamento (se applicabile)
- i dati personali, o le categorie di dati, ottenuti (se non ottenuti direttamente dall'utente)
- i destinatari, o le categorie di destinatari, dei dati personali (i dati personali saranno condivisi con altri soggetti?)
- i dettagli sui trasferimenti dei dati personali verso eventuali paesi terzi o organizzazioni internazionali (se applicabili)
- per quanto tempo vengono conservati i dati (periodo di conservazione)
- i diritti che possono essere esercitati dall'utente (es. diritto di accesso, diritto all'oblio, diritto di rettifica, ecc.)
- il diritto di revocare il consenso (se applicabile)
- il diritto dell'utente di fare reclamo all'autorità per la protezione dei dati personali
- la fonte dei dati personali (se i dati personali non sono ottenuti direttamente dall'utente)
- i dettagli sull'esistenza di processi decisionali automatizzati, inclusa la profilazione (se applicabile).

2.1.2. Limitazione delle finalità

Il principio della limitazione delle finalità prevede che le aziende o gli enti devono definire chiaramente una finalità specifica per ciascuna delle loro attività di trattamento dei dati, prima di iniziare. Questo requisito mira a fornire trasparenza, prevedibilità e controllo dell'utente. Qualsiasi trattamento di dati personali deve essere effettuato per una determinata finalità ben definita o per finalità ulteriori, determinate, compatibili con quella originaria. Il trattamento dei dati personali per finalità indefinite e/o illimitate è pertanto illecito.

Ogni nuova finalità del trattamento di dati personali non compatibile con la finalità originaria deve avere una sua particolare base giuridica e non può fondarsi sul fatto che i dati siano stati inizialmente acquisiti o trattati per un'altra finalità legittima.

Per esempio: Se si concede a Facebook il consenso a utilizzare la funzione di riconoscimento facciale al fine di individuare immagini e video all'interno della sua piattaforma, ciò non significa che Facebook possa utilizzare questi dati allo scopo di fornire pubblicità mirate basate su questi dati personali. Avrà bisogno di una base legale separata (ad es. consenso) per questo.

2.1.3. Minimizzazione dei dati

Le aziende e le organizzazioni possono elaborare solo i dati personali di cui hanno effettivamente bisogno per raggiungere lo scopo specificato, non di più. Ciò significa che dovranno rivedere regolarmente i dati che archiviano per eliminare tutto ciò di cui non hanno bisogno.

2.1.4. Precisione

Le aziende e le organizzazioni devono adottare misure ragionevoli per assicurarsi che i dati personali in loro possesso siano corretti e non fuorvianti. Ciò implica che dovranno mantenere aggiornati i dati personali, rettificandoli o cancellandoli, ove necessario.

2.1.5. Limitazione dell'archiviazione

I dati personali non possono essere conservati per sempre. Le aziende e le organizzazioni devono eliminare o rendere anonimi i dati personali non appena non ne hanno più bisogno per raggiungere le finalità per le quali quei dati sono stati raccolti. Le aziende e le organizzazioni devono riflettere in anticipo su quanto tempo desiderano conservare i dati personali dei loro utenti e se questo periodo di tempo è giustificabile, il che dipenderà dalle finalità del trattamento. Le informazioni su questo devono essere contenute nelle informative sulla privacy.

2.1.6. Integrità e riservatezza (sicurezza dei dati)

La protezione dei dati personali contro l'elaborazione non autorizzata o illecita, la perdita accidentale, la distruzione o il danneggiamento è al centro di questo principio di integrità e riservatezza (sicurezza dei dati). Il principio di sicurezza dei dati mira a evitare effetti negativi per l'utente obbligando l'implementazione di misure tecniche (es. crittografia, pseudonimizzazione) e/o organizzative (es. assicurarsi che i dati personali non siano disponibili a tutti all'interno di un'organizzazione, ma solo a coloro che devono lavorare con quei dati).

2.1.7. Responsabilità

Il principio di responsabilità richiede che le aziende o le organizzazioni si assumano la responsabilità di ciò che fanno con i dati personali dei loro utenti e di come si conformano al GDPR. Alla luce di ciò, devono mettere in atto misure e registrazioni che consentano loro di dimostrare la conformità quando richiesto.

I diritti dell'utente

Nella società digitalizzata attuale è importante conoscere i propri diritti dal punto di vista della protezione dei dati.

3.1. Il diritto ad essere informati

Le aziende e le organizzazioni devono informare gli utenti sulla raccolta e l'utilizzo dei loro dati personali. Ciò è legato al principio di trasparenza del GDPR. (Si veda il par. 2.1.1. (C) su quali informazioni dovrebbero essere fornite).

Le informazioni devono essere comunicate:

- Nel momento stesso in cui vengono raccolti i dati personali
- al più tardi entro un mese dopo aver ottenuto i dati, nel caso in cui questi siano stati ottenuti in modo indiretto

Le informazioni devono essere concise, trasparenti, intelligibili, facilmente accessibili e devono utilizzare un linguaggio chiaro e semplice. Queste informazioni sono fornite principalmente tramite una politica sulla privacy.

3.2. Il diritto di accesso

Ciascuno ha il diritto di accedere ai propri dati personali, detenuti da una società o organizzazione. In pratica, ciò significa che si possono ottenere le seguenti informazioni:

- Se la società o l'organizzazione stia elaborando o meno i dati personali dell'utente
- Una copia dei dati (generalmente in modo gratuito)
- Informazioni aggiuntive: le aziende o le organizzazioni devono fornire all'utente le stesse informazioni richieste dall'informativa sulla privacy (si veda 2.1.1.(c)).

L'esercizio di questo diritto aiuta l'utente a comprendere come e perché le aziende o le organizzazioni stanno utilizzando i suoi dati e a verificare se lo stanno facendo in conformità con il GDPR.

È possibile che l'azienda o l'organizzazione rifiuti l'accesso quando la richiesta è manifestamente infondata (per es. se è palesemente fatta solo per molestare l'azienda) o eccessiva (per es. se si sovrappone ad altre richieste). Le ragioni del rifiuto devono essere comunicate in modo chiaro. Le aziende e le organizzazioni hanno un mese per rispondere alla richiesta.

3.3. Il diritto alla cancellazione ("il diritto all'oblio")

Il GDPR garantisce all'utente il diritto alla cancellazione dei suoi dati personali. Questo diritto è legato ai principi di minimizzazione e accuratezza dei dati, e obbliga le aziende e le organizzazioni a cancellare i dati personali in determinate occasioni. Si può esercitare il diritto alla cancellazione quando:

- i dati personali dell'utente non sono più necessari allo scopo per il quale sono stati raccolti dalla società o dall'ente;
- quando la società o l'organizzazione fa affidamento sul consenso dell'utente come base legale per il mantenimento dei dati e questi desideri revocare il suo consenso;



- Quando la società o l'organizzazione fa affidamento su interessi legittimi come base legale per il trattamento, l'utente può opporsi al trattamento dei suoi dati e, se non esiste quell'interesse legittimo prevalente a continuare il trattamento, i dati saranno cancellati;
- Quando la società o l'organizzazione tratta i dati personali per inviare pubblicità diretta e l'utente si oppone a tale trattamento;
- Quando i dati personali dell'utente sono stati trattati in modo illecito (ovvero, senza fare riferimento in modo corretto a una fonte giuridicamente valida);
- Quando esiste un vincolo legale che obbliga alla cancellazione dei dati personali dell'utente;
- Quando i dati personali dell'utente sono stati raccolti quando era bambino per offrire servizi online.

Viene data particolare enfasi al diritto alla cancellazione se la richiesta riguarda dati raccolti su minori. Se il consenso al trattamento dei dati personali è stato originariamente prestato quando l'utente era un bambino (non pienamente consapevole dei rischi), può essere molto importante poter revocare il suo consenso e far rimuovere i dati personali. *(Probabilmente ogni studente può pensare a qualcosa che ha pubblicato online in passato, con cui non è più d'accordo o trova imbarazzante oggi)*

L'azienda o l'ente non è obbligata ad accogliere sempre (integralmente) la richiesta dell'utente in quanto in alcuni casi non si applica il diritto alla cancellazione (per es. se il trattamento è necessario per adempiere alla legge o quando il trattamento ha luogo a fini di archiviazione nel pubblico interesse o per ricerche scientifiche o storiche nel caso in cui la cancellazione comporti un grave pregiudizio alla ricerca). Una società o un ente può anche rifiutare l'esercizio del diritto alla cancellazione dell'utente quando la richiesta è manifestamente infondata o eccessiva (si veda 3.2).

Occorre rimarcare che, anche nell'esercizio del diritto all'oblio, sarà molto difficile (forse anche impossibile) cancellare completamente i dati personali da Internet. Questo perché i dati sono spesso (non) lecitamente condivisi da aziende e organizzazioni con altre parti che poi condividono nuovamente questi dati con altre parti e così via.



3.4. Il diritto alla rettifica

Il diritto alla rettifica stabilisce che si possono correggere eventuali errori nei dati personali dell'utente detenuti da società o enti: i dati personali inesatti possono essere rettificati e i dati incompleti possono essere completati. Questo diritto è chiaramente legato al principio di accuratezza a cui le aziende e le organizzazioni devono attenersi.

Anche in questo caso, le aziende e le organizzazioni non sono tenute a soddisfare sempre la richiesta dell'utente. Se ritengono che i dati personali dell'utente siano accurati, devono comunicarlo e spiegare la loro decisione. Un altro motivo per non accogliere (totalmente) la richiesta di rettifica può essere quando la richiesta appare manifestamente infondata o eccessiva (si veda 3.2).

3.5. Il diritto alla limitazione del trattamento

Questo diritto può essere esercitato in alternativa alla richiesta di cancellazione dei dati personali e consiste nel richiedere alla società o organizzazione l'interruzione del trattamento dei (alcuni dei) dati personali, di solito solo per un periodo di tempo limitato, mentre vengono risolte altre questioni. Questo diritto implica che l'azienda o l'organizzazione può solo memorizzare i dati personali dell'utente, senza utilizzarli ulteriormente.

Le aziende e le organizzazioni possono anche rifiutare la richiesta di limitazione del trattamento, con l'obbligo di fornire una spiegazione in merito. Uno dei motivi del rifiuto può essere ancora una volta il fatto che la richiesta è manifestamente infondata o eccessiva (cfr. 3.2).

3.6. Il diritto alla portabilità dei dati

Questo diritto garantisce la possibilità di ottenere e spostare i dati personali dell'utente – che sono stati forniti alla società o organizzazione – altrove. In pratica ciò significa che è possibile spostare, copiare o trasferire facilmente i propri dati personali da un ambiente digitale a un altro in modo sicuro e protetto e di uso comune, oppure chiedere all'azienda o all'organizzazione di farlo.

Questo diritto si applica solo quando la società o l'organizzazione si basa sul "consenso" o sulla "necessità contrattuale" come fonte lecita per il trattamento di tali dati personali, o quando i dati sono

trattati con mezzi automatizzati (vale a dire mediante programmi e strumenti informatici specializzati e per esempio non su carta).

Le aziende e le organizzazioni hanno anche la possibilità di rifiutare la richiesta di portabilità dei dati, con l'obbligo di fornire una spiegazione in merito. Uno dei motivi del rifiuto, anche in questo caso, può essere il fatto che la richiesta è manifestamente infondata o eccessiva (cfr. 3.2).

3.7. Diritto di opposizione

Il diritto di opposizione non è un diritto generico. Si può invocare il diritto di opposizione al trattamento dei dati personali in base a una situazione particolare e ai dati trattati allo scopo di fornire pubblicità diretta. Ciò consente di interrompere o impedire a società e organizzazioni di elaborare (parte dei) dati personali.

Il diritto di opporsi al trattamento per finalità di pubblicità diretta è un diritto assoluto, il che significa che le aziende e gli enti devono sempre accogliere tale richiesta. Quando il diritto di opposizione viene esercitato per un altro motivo, le aziende e le organizzazioni possono decidere di continuare a trattare i dati personali dell'utente nel caso in cui possano dimostrare che esiste un motivo impellente per farlo. Le aziende e le organizzazioni hanno altresì la possibilità di rifiutare la richiesta di opposizione al trattamento, con l'obbligo di fornire spiegazione. Uno dei motivi del rifiuto può essere sempre che la richiesta è manifestamente infondata o eccessiva (cfr. 3.2).

3.8. I diritti correlati al processo decisionale automatizzato, compresa la profilazione

La profilazione si riferisce alla valutazione degli aspetti personali dei dati al fine di fare previsioni sull'utente.

Per es.: il sito Web di un Social Media valuta determinate informazioni dell'utente (come l'età, il sesso, l'altezza) e in base a ciò lo classifica in un determinato gruppo correlato a contenuti per raccomandazioni o per scopi pubblicitari.



Il processo decisionale basato esclusivamente su mezzi automatizzati si riferisce alla situazione in cui la tecnologia stessa prende decisioni dell'utente, senza alcun coinvolgimento umano diretto (per es. attraverso gli algoritmi). Questo può essere fatto senza profilazione.

In base al GDPR, si ha il diritto di non essere soggetto a una decisione basata esclusivamente su mezzi automatizzati, se quella decisione produce effetti giuridici (vale a dire che i diritti legali vengono pregiudicati) che riguardano l'utente o incide in modo significativo su di esso (vale a dire che influenza condizioni, comportamenti o scelte). Poiché tali decisioni hanno probabilmente un impatto significativo sulla vita dell'utente (possono riguardare ad esempio l'affidabilità creditizia, il reclutamento elettronico, le prestazioni sul lavoro), è necessaria una protezione speciale.

Per es.: Le compagnie di assicurazione analizzano i post sui Social Media di (potenziali) clienti utilizzando un algoritmo alla ricerca di determinate parole e frasi che indicano un comportamento prudente o uno stato di buona salute per assegnare un livello di rischio al fine di calcolare il premio assicurativo.

3.8. In pratica

Quando si esercitano tali diritti, le aziende e le organizzazioni hanno un mese di tempo per rispondere alle richieste e per fornire informazioni a sostegno della loro decisione. Le richieste devono essere presentate all'azienda o all'organizzazione, verbalmente o per iscritto (solitamente tramite una e-mail o una specifica sezione del sito). L'esercizio di questi diritti deve essere facile tanto quanto lo è stato fornire i dati personali da parte dell'utente.

Pubblicità mirata/basata sui comportamenti

In passato, le aziende hanno investito principalmente in pubblicità televisiva e radiofonica. Ciò ha lo svantaggio che viene presentata a tutti la stessa pubblicità, che sia o meno di interesse per le persone, il che la rende poco efficiente. Oggi, i Social Media e i progressi tecnologici consentono alle aziende di scegliere di pubblicizzare i propri prodotti e servizi ai consumatori in modo mirato: ad





esempio, un annuncio per scarpe da corsa viene presentato solo agli utenti dei Social Media che vanno regolarmente a correre e, ad esempio, in giorni in cui non piove. Tali annunci mirati possono apparire sul feed notizie dei Social Media o su un lato di esso e possono essere riconosciuti dalla presenza di parole come "sponsorizzato".

Quali dati vengono utilizzati per la pubblicità?

1. I dati personali che vengono inseriti durante la creazione dell'account sui Social Media (ad es. età, luogo di residenza, data di nascita)
2. Qualsiasi cosa venga pubblicata sull'account di un utente dei Social Media, come foto, video e commenti. Per esempio: se si pubblica qualcosa come "Ho davvero fame in questo momento", è possibile che si riceva un annuncio da una catena di fast food;
3. Attività che si svolgono e si cercano al di fuori dei Social Media. Ad esempio, se si visita il sito Web di un determinato evento, si possono ricevere annunci pubblicitari su quell'evento o un evento simile. Tutto ciò è reso possibile dai "cookie".

I cookie sono piccoli file memorizzati sul tuo computer, laptop, smartphone o tablet al fine di tenere traccia dei siti web visitati. Si tenga presente che le aziende devono chiedere l'autorizzazione prima di utilizzare i cookie pubblicitari (ci sono anche altri tipi di cookie). Se non si desidera essere tracciato su diversi siti Web online, occorre ricordarsi di rifiutare tali cookie. L'uso dei cookie e di altre tecnologie di tracciamento è regolato dalle norme di ePrivacy e non dal GDPR.

È importante aggiungere che alcune società di Social Media possiedono più piattaforme e, quindi, possono utilizzare le informazioni ottenute su tutte le loro piattaforme (Facebook e Instagram per esempio);

4. La posizione dell'utente (in tempo reale). I Social Media possono persino rilevare dove si trova l'utente, in base al wifi e al localizzatore gps sul suo telefono. Ciò può comportare la ricezione di annunci pubblicitari per una determinata palestra, che si trovasse nelle immediate vicinanze.





Tutte le informazioni fin qui menzionate, vengono memorizzate ed elaborate da algoritmi, ovviamente, e non da esseri umani. Sulla base di questi dati, le aziende che scelgono di fare pubblicità sui Social Media possono scegliere un "gruppo target" (ad esempio ragazzi di 16 anni nella zona di Amsterdam a cui piace il calcio). La pubblicità giusta, al momento giusto e nel posto giusto, può influenzare seriamente il comportamento, a vantaggio delle aziende. Sebbene la pubblicità personalizzata non debba essere sempre percepita come una cosa negativa, bisognerebbe davvero essere cauti al riguardo. Soprattutto quando sono coinvolti dati sensibili (ad es. etnia, preferenze politiche, ecc.), questo tipo di pubblicità potrebbe essere ingannevole e i dati personali potrebbero anche essere utilizzati in modo improprio (ad es. prendere di mira con contenuti falsi, al fine di modificare o radicalizzare le preferenze politiche).

Cosa fare in caso di infrazioni?

Qualcuno ha condiviso illegalmente i tuoi dati personali? Ha creato un tuo falso profilo sui Social Media? Oppure, forse hai provato a esercitare uno dei tuoi diritti GDPR, ma non sei soddisfatto della risposta dell'azienda o dell'organizzazione?

Cosa fare in questi casi? In primo luogo, si può sempre chiedere alla persona che viola i diritti di protezione dei dati, di cancellare o correggere i dati personali in questione (ad esempio una foto, un profilo falso, i dettagli di contatto). Se non ottempera alla richiesta, è possibile rivolgersi alla piattaforma dei Social Media per far eliminare o correggere i dati personali in questione. Se anche questi passaggi non vengono soddisfatti, si può presentare un reclamo all'autorità nazionale per la protezione dei dati. (Un'altra opzione è quella di far valere i propri diritti attraverso un ricorso giurisdizionale).

Ogni paese dell'UE ha la propria autorità per la protezione dei dati. Si può trovare un elenco qui di seguito:

https://edpb.europa.eu/about-edpb/board/members_en

Le autorità per la protezione dei dati sono autorità pubbliche indipendenti che controllano e vigilano sulla corretta applicazione delle norme sulla protezione dei dati da parte di aziende e organizzazioni nel loro territorio. Forniscono anche consigli di esperti su questioni relative alla





protezione dei dati e gestiscono i reclami degli utenti. Le autorità possono emettere diffide, rimproveri, un divieto temporaneo o definitivo al trattamento e sanzioni (anche molto elevate).

Sui siti web di queste autorità per la protezione dei dati si può trovare come presentare un reclamo; questo può essere fatto per telefono, e-mail o tramite la compilazione di un modulo disponibile sul loro sito web.

Fonti

- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (General handbook on data protection)
- <https://www.youtube.com/watch?v=XVBHishpew8> (YouTube video: what is the GDPR?)
- https://www.youtube.com/watch?v=3fuirT_PwDI (YouTube video: GDPR explained)
- <https://www.youtube.com/watch?v=PVaVIOJniSQ&t=6s> (YouTube video: my data, my choice)
- https://cris.vub.be/files/27962258/arcades_teaching_handbook_final_EN.pdf (Free university of Brussels (VUB): The European Handbook for Teaching Privacy and Data Protection at schools)
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf (UK GOV: Data protection: a toolkit for schools)
- <https://www.gdpr.school/free-resources/> (useful GDPR sources for schools)
- https://edpb.europa.eu/about-edpb/board/members_en (List of national data protection authorities)
- <https://ico.org.uk/> (Website UK data protection authority ☞ a lot of information!)
- <https://en.mediawijs.be/poster-step-by-step-how-should-i-protect-my-privacy-on-social-media> (Mediawijs website „How do I protect my privacy on social media?”)
- https://www.youtube.com/results?search_query=internet+safety+tips+for+teens (YouTube video with internet safety tips for teens)
- <https://www.youtube.com/watch?v=yrln8nyVBLU> (YouTube: Safe Web Surfing: Top Tips for Kids and Teens Online)
- <https://mediawijs.be/nieuws/slag-gdpr-jouw-klas> (Mediawijs website about using the GDPR as part of your classes ☞ in Dutch)





Altre fonti

- o <https://d1afx9quaogywf.cloudfront.net/sites/default/files/Resources/School%20College%20Personal%20Data%20Advice%20and%20Guidance.pdf> (Information for schools to be GDPR compliant)
- o <https://www.youtube.com/watch?v=xtLR0Ey5-vo&t=76s> (YouTube video with information for schools to be GDPR compliant)
- o <https://www.youtube.com/watch?v=SpjpxspJNew&t=7s> (YouTube video with information for schools to be GDPR compliant)





Spunti di apprendimento

Accrescere la consapevolezza del GDPR è fondamentale

È essenziale che nell'era digitale di oggi gli studenti, gli insegnanti e tutto il personale scolastico siano a conoscenza del GDPR e della legislazione sulla protezione dei dati in generale. La quantità di dati personali che circolano online è enorme e continuerà a crescere, quindi tutti devono imparare a gestire i propri dati personali e quelli degli altri in modo responsabile.

Perché il GDPR è importante? Il valore dei dati personali!

Al giorno d'oggi, vengono prodotti grandi quantità di dati personali su base giornaliera, soprattutto online (ad es. pubblicando foto, video o aggiornamenti di stato sui Social Media, ma anche facendo acquisti online, leggendo un giornale online o giocando online: tutto questo genera dati che possono essere ricondotti all'utente). Alcune aziende, oltre a raccogliere ed elaborare dati personali per fornire un servizio specifico, mirano a raccogliere quanti più dati possibili per indirizzare in modo efficace la pubblicità. I dati personali hanno quindi un considerevole valore economico per aziende e organizzazioni. Inoltre, anche le autorità pubbliche sono interessate ai dati personali, perché sulla loro base possono fornire nuove informazioni. Ma anche le persone con intenzioni malevole, come gli hacker e ladri di identità sono alla ricerca di dati personali. Un utilizzo incontrollato dei dati personali può, di conseguenza, mettere in una posizione di potere aziende private, hacker e autorità pubbliche e mettere in una situazione indesiderabile l'utente.

Riflettere prima di condividere

Bisogna sempre riflettere attentamente quali dati personali si vanno a condividere con chi e come si possano ritrarre quando si postano sui Social Media (testo, immagini, video). È importante avere uno sguardo a lungo termine perché le informazioni possono fluttuare per sempre nel World Wide Web in quanto non è facile eliminare informazioni trasmesse su Internet. Prendersi cura delle





proprie impostazioni sulla privacy in modo che persone che non si conoscono non possano accedere a (gran parte dei) dei dati personali dell'utente. Anche esercitando il diritto alla cancellazione, infatti, è molto probabilmente che non possano cancellare tutte le tue tracce digitali.

Posso dare il mio consenso al trattamento dei miei dati personali?

Esiste un'età legale per i minori di acconsentire (o meno) al trattamento dei dati personali da parte di fornitori di servizi online. Questo limite di età può variare tra i 13 ei 16 anni a seconda dello Stato membro dell'UE.

La trasparenza, l'informazione è fondamentale

Uno dei principi fondamentali alla base del GDPR è il principio di trasparenza: le aziende e le organizzazioni devono essere chiare sul trattamento dei dati personali, su quali dati personali trattano, per quali motivi e come lo fanno, per quanto tempo ecc. Questo principio si traduce nel diritto degli utenti ad essere informati, che dovrebbe consentire di compiere scelte consapevoli sui propri dati personali. A tal fine il GDPR vuole rendere le persone consapevoli e responsabili di ciò che accade ai propri dati personali.

Come fare per sapere cosa sta facendo un'azienda o un'organizzazione con i dati personali raccolti?

La prima cosa che si dovrebbe fare per scoprire cosa stanno facendo le aziende o le organizzazioni con i dati personali raccolti è consultare l'informativa sulla privacy. Questa normativa deve avere una serie di elementi obbligatori. Se sembra che manchi qualcosa o qualcosa non è chiaro si può provare a contattare l'azienda o le organizzazioni per ulteriori chiarimenti.

Cosa fare nel caso in cui qualcuno stia abusando dei dati raccolti sui Social Media?

Opzione 1: contattare la persona/società/organizzazione che sta utilizzando i dati personali in modo illecito e chiedere loro di cancellare o correggere quei dati personali.





Opzione 2: contattare la piattaforma dei Social Media per richiedere la cancellazione o la correzione dei propri dati personali.

Opzione 3: presentare un reclamo all'autorità nazionale per la protezione dei dati (si veda il relativo sito web).

(Opzione 4: intraprendere le vie legali)



Infografiche

Si veda tutto il materiale didattico + l'infografica qui sotto.

What to do when someone is unlawfully using your personal data on social media?

1. **Contact the person/company/organisation** who is using your personal data in an unlawful manner and ask them to delete or correct your personal data.

2. **Contact the social media platform** in order to request the deletion or correction of your personal data.

3. File a complaint with your **national data protection authority** (see their website).

Attività con gli studenti

- Iniziare la lezione chiedendo agli studenti se sanno cosa sono i dati personali e perché pensano che sia importante proteggerli.
- Consentire agli studenti di controllare le loro impostazioni sulla privacy su Facebook (o su un altro sito di Social Media): chi è in grado di vedere le informazioni, e di che tipo? Successivamente si può aprire una discussione tra compagni di classe sul perché vogliono che le loro impostazioni siano in un certo modo o se desiderano cambiare le loro impostazioni.
- Chiedere agli studenti di individuare qual è il limite di età perché il consenso sia valido ai sensi del GDPR nel proprio paese di appartenenza. Questo può essere fatto attraverso il sito web dell'autorità nazionale per la protezione dei dati.

Si veda: https://edpb.europa.eu/about-edpb/board/members_en.

- Dopo aver fornito le informazioni sul principio di trasparenza, uno dei principi cardine del GDPR, e sul ruolo della normativa sulla privacy, gli studenti potrebbero prendere visione di tale normativa di un sito web di Social Media a loro scelta per osservare se contiene tutte le informazioni obbligatorie. Successivamente possono discuterne tra loro.
- Dopo aver spiegato agli studenti che hanno determinati diritti in relazione al trattamento dei loro dati personali, possono presentare una "richiesta di accesso" a Facebook (o un altro Social Media), per vedere quali dati personali Facebook detiene su di loro.

Si veda: <https://www.facebook.com/help/contact/2032834846972583>.

Valutazione

Si può facilmente valutare se gli studenti hanno compreso le informazioni sul GDPR sottoponendo questionari con brevi domande la cui risposta è vera o falsa, come negli esempi seguenti:

1. Un'immagine che ritrae una persona di spalle, completamente irriconoscibile, non è mai un dato personale ai sensi del GDPR? (**Falso**: l'immagine in quanto tale, senza altre informazioni, non è un dato personale, ma dal momento in cui qualcuno aggiunge il nome, l'indirizzo o il numero di telefono di questa persona all'immagine, essa diventa un dato personale in quanto è collegata a una persona specifica da quel momento in avanti)

2. La maggior parte dei siti Web e delle app che si utilizzano elaborano i dati personali. (**Vero**: lo scopo del trattamento dei dati personali può essere diverso. Ad esempio, solitamente il trattamento di nome e password è necessario per scopi di autenticazione. Spesso i dati personali come sesso, età, interessi vengono elaborati per finalità di marketing).

3. Il GDPR non tratta tutti i dati personali allo stesso modo. (**Vero**: la principale divisione operata nel GDPR è tra dati personali "generalisti" e categorie speciali di dati personali (es. salute, orientamento sessuale, religione). Questi ultimi devono essere trattati con maggiore attenzione a causa della loro natura sensibile (la condivisione di tali dati comporta un rischio maggiore in quanto potrebbero portare con più probabilità a conseguenze indesiderate, quali discriminazione, esclusione, ecc.) ed è per questo che, in linea di principio, il trattamento di questi dati è vietato (anche i dati relativi a reati e i dati relativi a minori sono oggetto di un regime speciale)

4. Una scuola pubblica online le schede di valutazione di ogni studente per consentire ai genitori di confrontare i risultati del proprio figlio con quelli dei compagni di classe. Questo è consentito perché è nell'interesse del bambino. (**Falso**: non è così che funziona. Per ogni trattamento in corso, un'azienda o un'altra organizzazione, compresa una scuola, deve fare riferimento a una base legale valida determinata nel GDPR. Poiché ciò potrebbe potenzialmente influire negativamente sui bambini, l'unico modo in cui una scuola può farlo è con il consenso per ogni bambino e/o genitore.

5. Nel trattamento dei dati personali è sempre richiesto il consenso dell'interessato. (**Falso**: il consenso è solo una delle basi giuridiche su cui le società e altri organismi possono fare riferimento

per giustificare le proprie attività di trattamento dei dati (cfr. artt. 6 e 9 GDPR). Infatti, il consenso non è sempre necessario. Per ogni attività di trattamento è necessario scegliere sempre la base giuridica di riferimento per il trattamento più adatta alla situazione.

6. In passato, hai acconsentito alla pubblicazione di una tua foto sulla pagina dei Social Media di un'azienda, ma ora questa foto non ti piace più. Sfortunatamente, poiché in passato hai dato il tuo consenso a pubblicare la foto, non puoi farci più nulla. (**Falso**: puoi sempre ritirare il tuo consenso, il che significa che l'azienda dovrà eliminare l'immagine)

7. Alcuni studenti sono stati fotografati in classe e hanno fornito il consenso all'utilizzo di quella foto nella presentazione della scuola. Successivamente la scuola ha deciso di condividere questo opuscolo sui propri Social Media. Ciò è consentito dal GDPR. (**Falso**: il consenso deve essere prestato in modo specifico e non può essere raggruppato per più finalità. Ciò significa che la scuola dovrebbe aver ottenuto un consenso separato ed esplicito per l'utilizzo dell'opuscolo sui propri canali social).

8. L'obiettivo principale del GDPR è limitare la pubblicità online. (**Falso**: nella società digitalizzata odierna, in cui i dati personali sono super preziosi, il GDPR mira a restituire ai cittadini il controllo sui propri dati personali fornendo loro maggiore protezione e diritti; in più, poiché si applica direttamente in tutta l'UE, armonizza 27 diverse giurisdizioni sulla protezione dei dati).

9. Quando salvi sul telefono una foto di un'altra persona che hai trovato su Instagram, solo per mostrare al tuo parrucchiere il taglio di capelli che vorresti, il GDPR non si applica. (**Vero**: il GDPR non si applica alle attività personali e domestiche)

10. La pubblicità mirata sui comportamenti è consentita sui Social Media solo se hai acconsentito a ciò? (**Vero**: per la pubblicità basata sul tuo comportamento di navigazione, è necessario l'uso dei cookie. Affinché i siti web memorizzino questi cookie sul tuo dispositivo, è necessario il tuo preventivo consenso, in base al regolamento ePrivacy, non al GDPR. Inoltre, le aziende dovrebbero fornirti sempre la possibilità di revocare tale consenso).