Ciclo E-commerce

II° incontro
La protezione dei dati personali nell'ambito dell'e-commerce

24 maggio 2021

Avv. Nicolò Maggiora - Avv. Emilio Villano

II incontro - : a protezione dei dati personali nell'ambito dell'e-commerce

Programma

- Quadro normativo (Regolamento UE 679/2016 GDPR - Codice Privacy- aggiornamento Regolamento e-privacy- cookies law)
- Ambito applicativo, definizione di "dato personale", principi chiave del GDPR, i soggetti, basi giuridiche: focus sul sito e-commerce
- Obblighi e responsabilità del titolare (procedure, informative, contratti)
- DPO: funzioni e responsabilità
- Prevenzione e segnalazione del *data breach*
- Ispezioni del Garante e profili sanzionatori (analisi casistiche)

FONTI GIURIDICHE

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) – («GDPR» o «RGPD»)

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (il «**Codice Privacy**»)

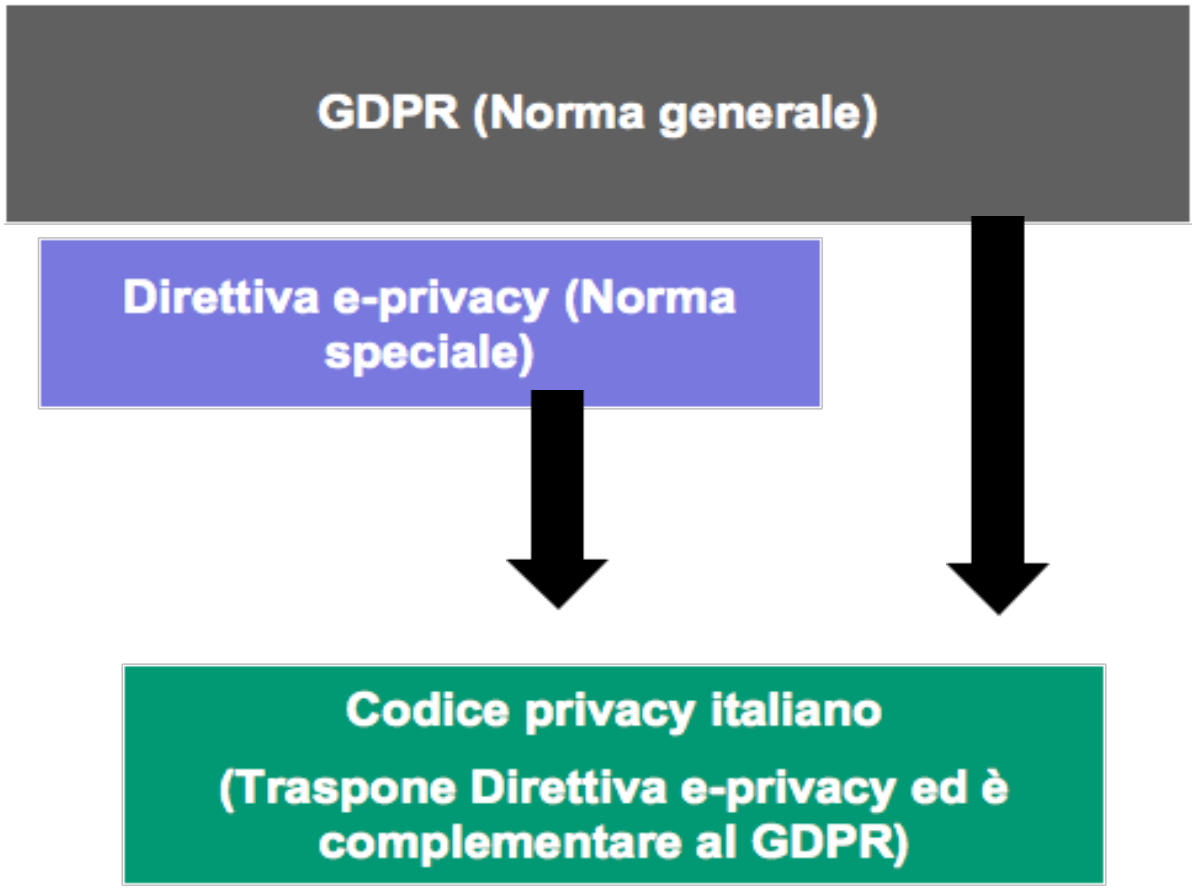
DIRETTIVA 2002/58/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (la «Direttiva e-privacy»)

DIRETTIVA E-PRIVACY

Il panorama normativo:

In attesa del Regolamento sulla vita privata e le comunicazioni elettroniche (il «**Regolamento e-privacy**») che andrà a sostituire la direttiva e-privacy

- Prevale sul GDPR rispetto alle materie da essa regolate
- La disciplina relativa all'utilizzo dei cookies è contenuta nella Direttiva e-privacy e deve, comunque, essere conforme ai dettami del GDPR
- La direttiva e-Privacy - più specificamente l'articolo 5 (3) - richiede il consenso informato preliminare per l'archiviazione o l'accesso alle informazioni memorizzate sull'apparecchiatura terminale dell'utente. In altre parole, occorre chiedere agli utenti se accettano la maggior parte dei cookies e tecnologie simili (ad esempio web beacon, cookie Flash, ecc.) prima che il sito inizi a utilizzarli.


GDPR (Norma generale)
Direttiva e-privacy (Norma speciale)
Codice privacy italiano
(Traspone Direttiva e-privacy ed è complementare al GDPR)

GDPR in generale

- Evoluzione storica
- Applicazione diretta in tutti gli Stati Membri dell'UE (non servono norme nazionali di trasposizione)
- Si applica solo ai «dati personali»
- Soggetti coinvolti (titolare, interessato, responsabile esterno, DPO)
- Basi giuridiche - Finalità
- Principi: legalità, correttezza, trasparenza, limitazione, minimizzazione, accuratezza, conservazione limitata, sicurezza e responsabilità
- *Privacy by Design and by* Default - principio dell'accountability
- Nozione di «trattamento»
- Nozione di «trasferimento verso Paesi terzi»
- Sanzioni pesanti e commisurate al fatturato delle aziende

GDPR in generale

- La *leggenda metropolitana* del «consenso». Le altre basi giuridiche per il trattamento di dati personali senza consenso e la natura residuale dello stesso
- Marketing: consenso/legittimo interesse/soft spam (cfr. Garante vs TIM)
- La profilazione commerciale
- Controlli e sanzioni

I PRINCIPI

Principio di accountability

- Uno dei pilastri su cui si fonda l'impianto normativo del GDPR.
- Responsabilizzare. Responsabilizzare il titolare di un trattamento dati che (così facendo) non è più mero esecutore di un elenco di misure imposte ad una norma, ma diviene responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate per salvaguardare i dati che tratta.
- *Art.32, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento* ***mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*** *…".*

Principi generali del GDPR

I dati personali devono essere protetti e tutelati sulla base dei seguenti principi:

- **liceità**, nel senso che i dati devono essere trattati in modo lecito, corretto e trasparente;
- **limitazione della finalità**: i dati devono essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- **minimizzazione dei dati**: i dati trattati devono essere solamente quelli indispensabili, quindi pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**, nel senso che devono essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- **limitazione della conservazione**: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati;
- **integrità e riservatezza**: i dati sono trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

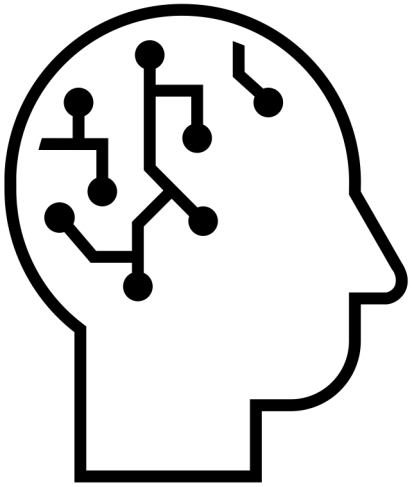
Privacy by design e Privacy by default

- Principio di necessità del trattamento fin dalla progettazione del sistema, tecnologico ed organizzativo, con cui intendono trattare i dati, in un approccio di prevenzione ex ante e non di risoluzione ex post dei rischi connessi al trattamento.
- Si va verso la predisposizione di un **modello organizzativo per la protezione dei dati**
-
- L'utente con i suoi diritti deve essere posto al centro del sistema di gestione dei dati mirando ad una tutela effettiva da un punto di vista sostanziale e non solo formale.
-
- COME: approccio basato sulla valutazione del rischio; utilizzo di tecniche di pseudonominazione o di minimizzazione dei dati; deve essere garantita la massima funzionalità sia in termini di tutela dei dati personali sia di sicurezza.

- Protezione dei dati per impostazione predefinita: le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità e per il periodo strettamente necessario a tali fini.
- Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti. in modo che l'interessato riceva un alto livello di protezione anche se non si attiva per limitare la raccolta dei dati (es. tramite opt out).

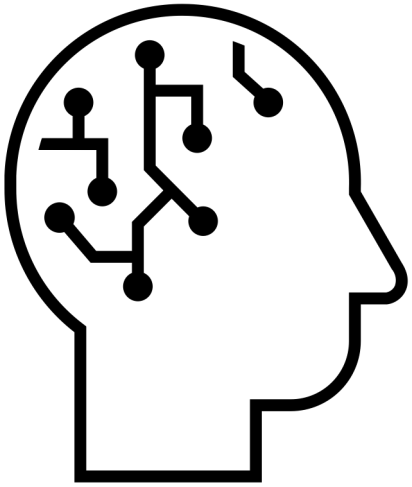
I SOGGETTI

Interessato



persona fisica alla quale i dati personali si riferiscono

Titolare del Trattamento

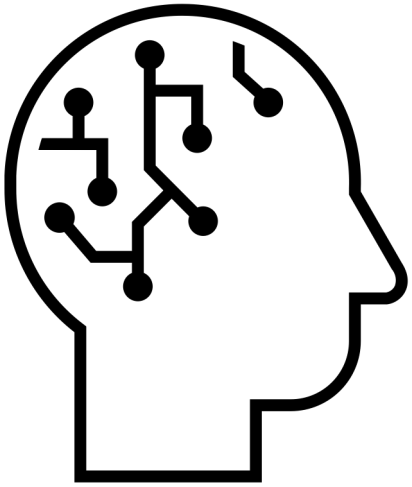


Il Titolare del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro ente che, singolarmente o insieme ad altri, determina nel finalità e I mezzi del trattamento di dart personali.

Il Titolare del trattamento decide il come ed il perché debbano essere trattati i dati personali. Il Titolare del trattamento non è il soggetto che gestisce I dati ma è il soggetto che decide il motive e le modalità del trattamento.

Il Titolare del trattamento mette in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento (*accountability).*

Responsabile esterno ex art. 28 GDPR



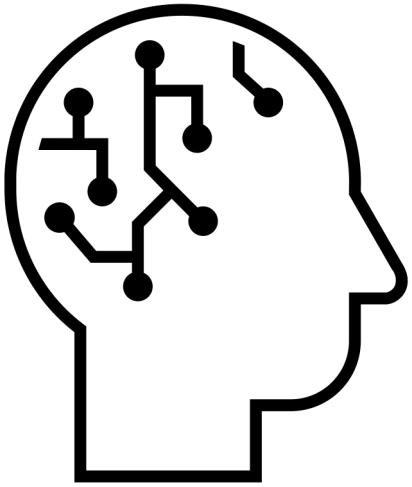
Il responsabile **esterno** del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento a cui è legato sulla base di un **contratto.** Il contratto deve prevedere, in particolare, che il responsabile esterno del trattamento:

✓Tratti I dati personali soltanto su istruzione documentata del titolare del trattamento

✓Garantisca che le persona autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza

✓Adotti tutte le misure richieste ai sensi dell'art. 32 (sicurezza del trattamento)

Incaricati interni al trattamento



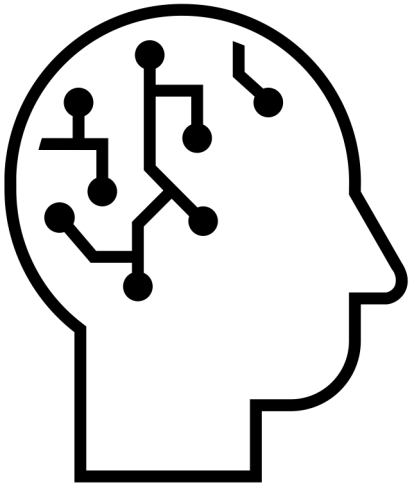
Il GDPR non prevede la figura dell'**incaricato**, ma non ne esclude la nomina, facendo riferimento a **persone autorizzate** al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

Incaricato, o autorizzato, è il **soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali**. L'autorizzato può operare alle dipendenze del titolare, o del responsabile esterno se nominato. Ovviamente gli autorizzati possono essere organizzati con **diversi livelli di delega.** L'autorizzato deve, ovviamente, attenersi strettamente alle istruzioni ricevute, e non deve avere alcuna autonomia (altrimenti è "responsabile").

Il GDPR non prevede l'obbligo di nomina o designazione espressa, ma è fondamentale **fornire agli autorizzati le istruzioni operative** (art. 29 GDPR), compreso gli obblighi inerenti le misure di sicurezza, e che sia fornita loro la **necessaria formazione**. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.

La designazione degli autorizzati può avvenire anche con unico atto per più persone. L'eventuale designazione non necessita di firma per accettazione, anche se è utile una **firma per presa visione**, quale prova della conoscenza dell'incarico e delle istruzioni fornite.

Amministratore di sistema



Non è espressamente nominato dal GDPR ma la sua figura implicitamente richiamata, in alcune norme, per le sue specifiche competenze tecniche, laddove al titolare del trattamento e/o all'eventuale responsabile nominato, spetta il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio

Si occupa della gestione e della manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

L’Informativa all’Interessato

L’Informativa deve essere:

- ✓Concisa
- ✓Trasparente
- ✓Comprensibile
- ✓Facilmente accessibile
- ✓Semplice
- ✓Chiara (specie se rivolta a minori)

Le informazioni devono essere fornite per iscritto o con altri mezzi, se del caso in formato elettronico.

Andrà precisato il periodo di conservazione dei dati personali oppure, se non è possibile i criteri utilizzare per determinare questo periodo.

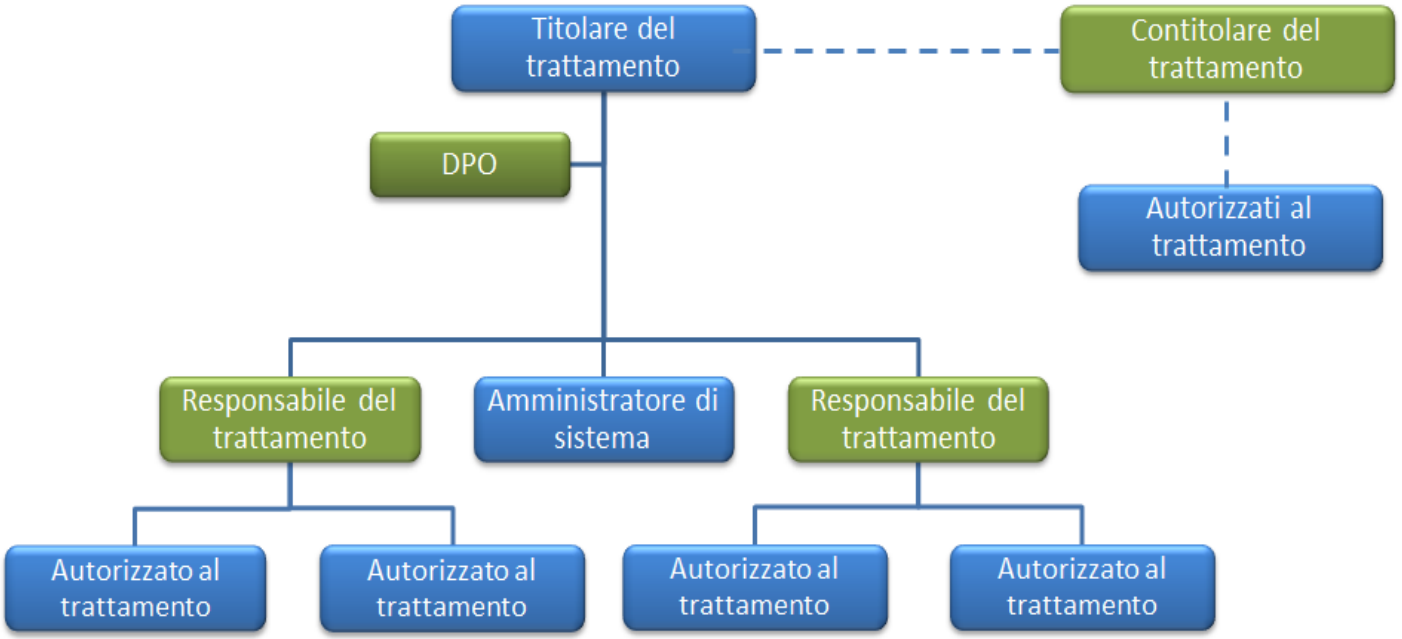
Se i dati non sono stati raccolti presso l’interessato andrà indicata l’origine del dato.

L’Informativa all’Interessato

In caso di raccolta dei dati presso l’Interessato, l’Informativa dovrà contenere:

- ✓**I dati del Titolare del Trattamento**
- ✓**Il nominativo del DPO**
- ✓**Finalità e base giuridica del trattamento**
- ✓**Destinatario dei dati**
- ✓**Intenzione di trasferire i dati in un paese extra UE**
- ✓**Periodo di conservazione dei dati**
- ✓**Diritti degli interessati**
- ✓**Diritto di revocare il consenso**
- ✓**Diritto di proporre reclamo**
- ✓**Conseguenze della mancata comunicazione dei dati**
- ✓**Esistenza di processi decisionali automatizzati (es. profilazione)**

Organigramma privacy



Designazione del Data Protection Officer

Il Regolamento introduce la figura del Responsabile per la protezione dei dai personali o *Data Protection Officer*.

Il DPO non è mai responsabile del trattamento dei dati. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Le aziende che dovranno dotarsi del DPO sono:

✓Tutte le imprese e le attività che operano nel settore pubblico

✓Tutte le imprese che trattino dati in modo rilevante

Il Dpo deve essere designato come soggetto referente del Garante e deve poter operare con ampia autonomia e competenza professionale.

Diritti degli Interessati

Diritti degli interessati

Quali sono

Nell'ambito del trattamento dei propri dati personali gli interessati hanno i seguenti diritti:

- ✓ Diritto di accesso
- ✓ Diritto alla rettifica
- ✓ Diritto all'oblio (cancellazione)
- ✓ Diritto alla limitazione del trattamento
- ✓ Diritto alla portabilità dei dati
- ✓ Diritto di opposizione

Il Titolare deve rispondere all'interessato entro 1 mese dall'esercizio di uno dei diritti sopra indicati.

Inosservanza dei diritti degli interessati

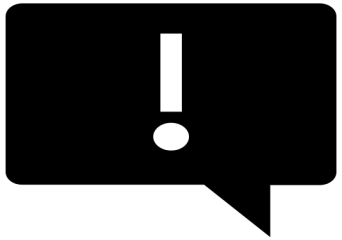
Sanzioni

Fino a 20,000 euro o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente

Procedura di *data breach*

Data breach

Distruzione, perdita, modifica, rivelazione non autorizzata o l'accesso accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati



- In caso di *data breach,* il Titolare deve:

✓notificare la violazione all'Autorità di controllo entro 72 ore dal fatto;

✓segnalare la violazione al diretto interessato senza ingiustificato ritardo;

✓aggiornare il registro dei trattamenti.

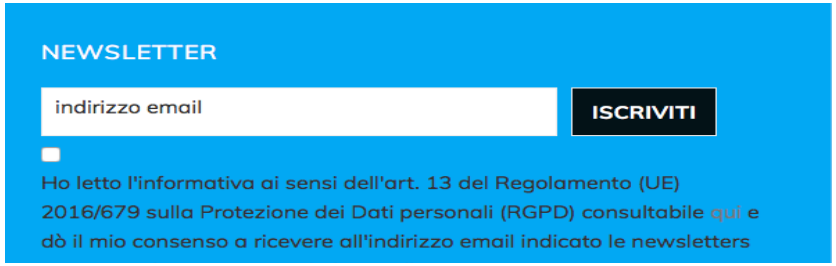
GDPR / e-commerce

- Fornire informativa chiara e completa e corrispondente alla realtà
- Rispetto dei principi del GDPR (minimizzazione limitazione ecc)
- Ottenere e registrare il consenso preventivo (ove necessario) specifico per ogni finalità di trattamento (no caselle spuntate, no consenso generalizzato)
- Misure di sicurezza adeguate

GDPR / e-commerce

NO

SI



Cookies

- La disciplina relativa all'utilizzo dei **cookies** è contenuta nella Direttiva e-privacy che in Italia è stata recepita nel Codice Privacy
- I cookies sono una sorta di "memoria" attraverso la quale un sito web riesce a riconoscere uno specifico utente e ad associagli delle informazioni di varia natura e per differenti finalità
- La direttiva e-Privacy - più specificamente l'articolo 5 (3) - richiede il **consenso informato specifico e preliminare** per l'archiviazione o l'accesso alle informazioni memorizzate sull'apparecchiatura terminale dell'utente. In altre parole, occorre chiedere agli utenti se accettano la maggior parte dei cookies e tecnologie simili (ad esempio web beacon, cookie Flash, ecc.) prima che il sito inizi a utilizzarli.

Cookies

Cookie Tecnici: utilizzati per migliorare il funzionamento e la fruizione del sito
SI informativa, NO consenso preventivo dell'utente

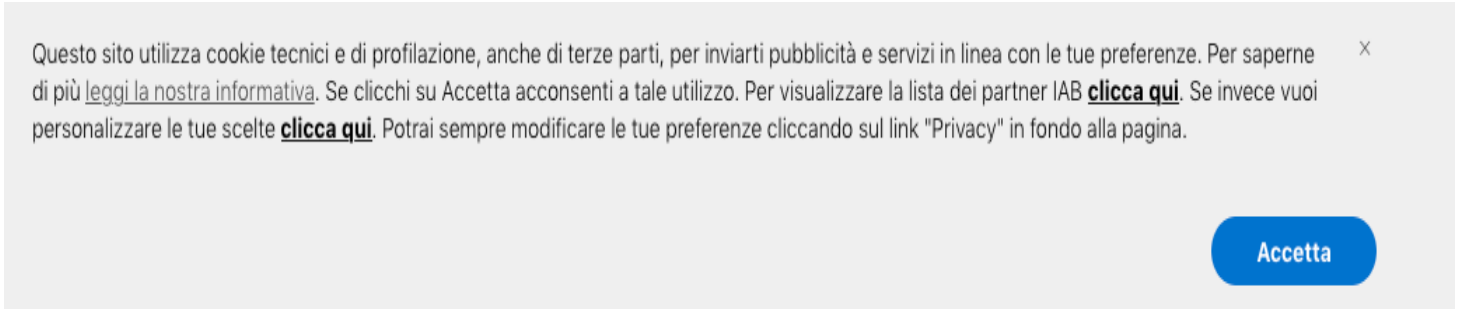
Cookie di Profilazione: utilizzati per creare profili degli utenti sulla base delle loro preferenze manifestate durante la navigazione
Tra questi ci sono: cookie di rilevamento (tracking cookies), cookie di profilazione, cookie di analisi, cookie di terze parti …
SI informativa, SI consenso preventivo dell'utente

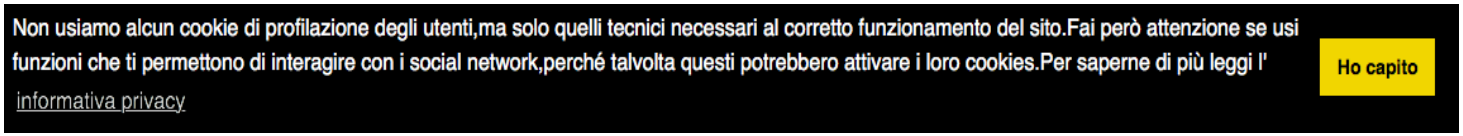
- Secondo il WP29 (oggi European Data Protection Board) non è necessario il consenso per i seguenti cookies:

1. *user-input cookies (session-id) such as first-party cookies to keep track of the user's input when filling online forms, shopping carts, etc., for the duration of a session or persistent cookies limited to a few hours in some cases*
2. *authentication cookies, to identify the user once he has logged in, for the duration of a session*
3. *user-centric security cookies, used to detect authentication abuses, for a limited persistent duration*
4. *multimedia content player cookies, used to store technical data to play back video or audio content, for the duration of a session*
5. *load-balancing cookies, for the duration of session*
6. *user-interface customisation cookies such as language or font preferences, for the duration of a session (or slightly longer)*
7. *third-party social plug-in content-sharing cookies, for logged-in members of a social network.*

Cookie e privacy: istruzioni per l'uso

https://www.youtube.com/watch?v=Mut-YXSExnw





Privacy Shield

Problema

- La **sentenza C-311/18 del 16 luglio 2020 (**Schrems II) della Corte di Giustizia UE, ha invalidato il "Privacy Shield", ovvero l'accordo per il trasferimento di dati personali tra Europa e Stati Uniti.

- La ragione alla base di questa decisione è che l'attuale livello di protezione dei dati personali statunitense non può essere considerato equivalente a quello del GDPR.

- Il Privacy Shield non costituisce più una base valida per trasferire i dati dell'UE negli Stati Uniti.

Privacy Shield

Cosa fare

- ❑ Verificare i trasferimenti verso gli Stati Uniti e le base giuridiche

- ❑ Se ci si basava sul PS cercare alternative, quali:
  - Clausole contrattuali standard
  - Binding Corporate Rules
  - Consenso esplicito e altre eccezioni ai sensi dell'articolo 49 del GDPR (trasferimento di dati necessario all'esecuzione di un contratto di cui è parte l'interessato)
  - Riconsiderare il trasferimento dei dati negli Stati Uniti

- ❑ Aggiornamento documentazione privacy (Registro dei Trattamenti informative ecc)

- ❑ Monitorare attentamente le attività delle Autorità di controllo competenti circa ulteriori interpretazioni e consigli pratici

I controlli e le sanzioni

Chi effettua i controlli

Da sempre, Guardia di finanza e Autorità Garante collaborano tramite attività ispettive de di controllo per la tutela della *privacy.*

In sede ispettiva, sarà fondamentale il rispetto del principio di *accountability* (responsabilizzazione).

In altre parole, l'Azienda o il Professionista dovrà dimostrare cosa è stato fatto e cosa non, allegando i motivi del mancato adempimento.

Non soltanto bisognerà trattare i dati secondo le regole previste dal GDPR ma bisognerà dimostrare di essere consapevoli delle modalità di trattamento e di conservazione degli stessi. I Titolari del trattamento dovranno render conto in maniera responsabile di quanto fatto.

Cosa viene verificato

✓Nomina del DPO

✓Controlli nelle misure previste in caso di *data breach* (da intendere come tutti quei casi di perdita accidentale e occasionale di dati, come furto di un pc, hardisk ecc.)

✓Registro dei trattamenti: sarà la base dell'attività, il punto dal quale la Guardia di finanza partirà per valutare le misure per la tutela della privacy messe in atto dal Titolare

✓Misure minime di sicurezza, come definite dall'all. B del codice della privacy: Credenziali di autenticazione (password); Protezione contro il rischio di intrusione (firewall e antivirus); *Back up* dei dati; custodia della documentazione.

Sanzioni 2020

- In Italia 35 sanzioni per un importo totale di € 58 milioni (fonte Report Federprivacy 2020)

- Il Garante della Privacy ha sanzionato Wind Tre Spa per circa 17 milioni di euro per "*numerosi trattamenti illeciti di dati, legati prevalentemente ad attività promozionali*", mentre un altro gestore telefonico, Iliad, "*che è stato trovato carente sotto altri profili, in particolare in merito alle modalità di accesso dei propri dipendenti ai dati di traffico*", è stato sanzionato per 800.000 euro.

- Duemila euro di multa per aver diffuso i dati personali degli alunni affiggendoli sulla porta della scuola.

- Garante per la protezione dati personali ha ordinato a Vodafone il pagamento di una sanzione di oltre 12 milioni e 250 mila euro per aver trattato in modo illecito i dati personali di milioni di utenti a fini di telemarketing.

- https://www.enforcementtracker.com/

tab.2 – Elenco delle nazioni irrogratrici classificate in base al valore economico delle sanzioni

Nazione	Importo (€)	Numero di sanzioni	Importo medio della sanzione (€)
Francia	138.316.300	8	17.289.539
Italia	58.176.601	35	1.662.188
Regno Unito	45.067.000	5	9.013.400
Germania	37.398.708	3	12.466.236
Svezia	14.278.800	15	951.920
Spagna	8.080.710	133	60.757
Paesi Bassi	1.355.725	3	451.908
Ungheria	1.002.525	13	77.117
Norvegia	805.200	11	73.200
Belgio	798.000	14	57.000
Irlanda	630.000	4	157.500
Polonia	531.698	9	59.078
Repubblica Ceca	312.178	8	39.022
Finlandia	207.500	5	41.500
Danimarca	202.300	6	33.717
Romania	184.650	26	7.102
Estonia	148.500	3	49.500
Slovacchia	107.000	4	26.750
Austria	100.750	3	33.583
Malta	64.500	11	5.864
Grecia	45.000	7	6.429
Cipro	32.000	5	6.400
Islanda	29.600	2	14.800
Lettonia	21.250	2	10.625
Lituania	15.000	1	15.000
Bulgaria	12.230	4	3.058
Croazia	N.D.	1	N.D.
Portogallo	0	0	0
Slovenia	0	0	0
Liechtenstein	0	0	0
Lussemburgo	0	0	0
Totale	**307.923.725**	**341**	**903.002**

tab.3 – Elenco delle nazioni irrogratrici classificate in base al numero di sanzione

Nazione	Numero di sanzioni	Importo (€)	Importo medio della sanzione (€)
Spagna	133	8.080.710	60.757
Italia	35	58.176.601	1.662.188
Romania	26	184.650	7.102
Svezia	15	14.278.800	951.920
Belgio	14	798.000	57.000
Ungheria	13	1.002.525	77.117
Norvegia	11	805.200	73.200
Malta	11	64.500	5.864
Polonia	9	531.698	59.078
Francia	8	138.316.300	17.289.539
Repubblica Ceca	8	312.178	39.022
Grecia	7	45.000	6.429
Danimarca	6	202.300	33.717
Regno Unito	5	45.067.000	9.013.400
Finlandia	5	207.500	41.500
Cipro	5	32.000	6.400
Irlanda	4	630.000	157.500
Slovacchia	4	107.000	26.750
Bulgaria	4	12.230	3.058
Germania	3	37.398.708	12.466.236
Paesi Bassi	3	1.355.725	451.908
Estonia	3	148.500	49.500
Austria	3	100.750	33.583
Islanda	2	29.600	14.800
Lettonia	2	21.250	10.625
Lituania	1	15.000	15.000
Croazia	1	N.D.	N.D.
Portogallo	0	0	0
Slovenia	0	0	0
Liechtenstein	0	0	0
Lussemburgo	0	0	0
Totale	**341**	**307.923.725**	**903.002**

Il Web è solo uno strumento. Non dobbiamo incolparlo del nostro atteggiamento superficiale nei confronti del mondo in cui viviamo. La sua virtù è la brevità e la molteplicità delle informazioni; non ci può anche fornire concentrazione e profondità.
Alberto Manguel, La biblioteca di notte, 2006

Grazie!

Avv. Nicolò Maggiora – Avv. Emilio Villano

ELEXI Studio Legale
www.elexi.it