Trattamento dei dati sensibili Appunti

Trattamento dei dati sensibili (Università degli Studi di Milano)

ARGOMENTI TRATTATI A LEZIONE

GOOGLE ANALYTICS

Usando Analytics per raccogliere dati personali degli utenti ed esportarli negli Stati uniti. Il Garante ha accertato la violazione degli art 44 e 46 del GDPR in tema di trasferimento di dati personali.

Nel caso di Pseudoanonimizzazione dei dati, il dato pseudo anonimo è considerato come non anonimo.

La CNIL suggerisce l'integrazione di un Proxy ubicato in territorio europeo opportunamente configurato per consentire una anonimizzazione/ pseudo anonimizzazione ed aggregazione di dati ed assenza di trasferimenti di indirizzi IP.

Google Analytics 3 non è GDPR compliant, GA 4 pare lo sia al momento.

Pro: evita trasferimento dati verso USA Contro: pratica complessa

REPUTATION ECONOMY

La reputazione è frutto di un processo con il quale si richiamano a se informazioni attirando attenzioni al fine di generare fiducia.

Questo processo si definisce "auto-branding", evidenzia il contesto lavorativo di un soggetto attirando incarichi professionali.

L'identità digitale così creata diviene come merce sul mercato del lavoro funzionale alla acquisizione di nuovi incarichi. La creazione di un'identità digitale diviene una funzione per monetizzare attenzione e notorietà.

Valutando diversi fattori siamo in grado di definire un valore economico per l'identità digitale di un soggetto.

L'identità digitale spetta a persone fisiche, giuridiche, enti e personaggi di fantasia a cui si possono attribuire caratteristiche pressoché uniche.

DIRITTO D'AUTORE (L. 633/1941)

Il Diritto d'autore è l'istituto giuridico che ha lo scopo di tutelare i frutti dell'attività intellettuale mediante il riconoscimento di una serie di diritti (di carattere morale o patrimoniale) all'autore originario dell'opera.

L'esercizio in forma esclusiva di questi diritti da parte dell'autore permette di remunerarsi per un periodo di tempo attraverso lo sfruttamento commerciale dell'opera.

Diritto morale d'autore, nasce nel momento in cui l'opera creativa si manifesta. Forma di diritto la cui durata di tempo è illimitata. All'autore contraente di tale diritto spetta diritto di rivendicare la proprietà

NIST Cyber security Framework

Il **framework core** rappresenta la struttura del ciclo di vita del processo di gestione della cyber security, dal punto di vista tecnico che organizzativo.

Il Core è strutturato in function, category e subcategory.

Le function, concorrenti e continue, costituiscono le principali tematiche da affrontare per operare un'adeguata gestione del rischio cyber, e sono:

- Identify
- Protect
- Detect
- Respond
- Recover

I punti trattati dal NIST CSF vengono ripresi e rivisti dal Framework Nazionale per la cybersecurity, nel quale si aggiungono livelli di priorità, livelli di maturità e contestualizzazioni.

GDPR E SPIEGAZIONE DEGLI ARTICOLI

Art 4, 5, 6, 9, 10, 12 ,13, 14,15, 16. 17, 18, 20, 21, 22, 24, 25, 26, 28, 29, 30 ,32, 33, 34, 35, 37, 38, 39, trasferimento capo V, aut. Controllo da leggere, 68, 83

A CHI SI RIVOLGE IL GDPR?

Il GDPR è rivolto alle **organizzazioni costituite in Unione Europea**;
Alle persone giuridiche **con** sede in Unione Europea, indipendentemente dal fatto che i dati siano trattati all'interno o all'esterno dell'Unione.
Alle organizzazione che hanno **sede fuori dall'Unione europea, ma che trattano dati di persone situate all'interno dell'Unione Europea**.

Il regolamento prevale su eventuali norme in conflitto dei vari stati membri, compresi i regolamenti speciali.

Lo CNIL è l'autorità garante francese, ci si fa affidamento in caso in cui il garante italiano abbia dei buchi oppure ci siano dei pareri utili.

DIRITTI DELLA PERSONALITA'

Si intendono tutti quei diritti soggettivi ed assoluti volti a garantire le ragioni fondamentali della vita e dello sviluppo, fisico e morale, dell'esistenza della persona. Tali diritti non hanno carattere patrimoniale, sono inalienabili, intrasmissibili, irrinunziabili, imprescrittibili

DIRITTI ALL'IDENTITA' PERSONALE

Può essere definito come l'interesse di ogni persona a non vedere travisato o alterato all'esterno del proprio patrimonio intellettuale, politico, sociale, religioso, professionale, a causa dell'attribuzione di idee, opinioni o comportamenti differenti da quelli che l'interessato ritenga a priori. Altri diritti della persona sono il diritto al nome, alla privacy e riservatezza, all'oblio…

DIRITTI ALLA REPUTAZIONE vedi art 12

E' possibile definire il concetto di reputazione come:" la rappresentazione della personalità di un soggetto in una cerchia di consociati".
Secondo tale impostazione, essa viene lesa da quegli addebiti o offese che colpiscono un rapporto di stima esistente o fanno sorgere un rapporto di disistima". Altri diritti sono il diritto alla privacy, all'oblio, al nome…

DIRITTO ALLA PORTABILITA' vedi art 20

In termini generali – la possibilità di ricevere dal titolare del trattamento, cui si abbia fornito i propri dati personali, tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico, inoltre trasmettere i dati in quel formato ad un altro titolare del trattamento.

ART 4, DEFINIZIONI

DATO, una qualsiasi registrazione elementare nella memoria di un pc.

I dati personali sono:

1. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("**liceità, correttezza e trasparenza**")
2. Raccolti per finalità determinate, esplicite, legittime, in modo compatibile con le finalità (**limitazione delle finalità**)
3. Adeguati, pertinenti e limitati a quanto necessario alle finalità (**minimizzazione dei dati**)
4. Esatti e, se necessario, aggiornati (**esattezza**)
5. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore in relazione alle finalità per i quali sono trattati (**limitazione della conservazione**)
6. Trattati in maniera da garantire un'adeguata sicurezza dei dati personali compresa protezione, mediante misure tecniche e organizzative (**integrità e riservatezza**)

I DATI PERSONALI, si dividono in:

- **Personali semplici**;
- **Particolari**:
  - **Genetici**, dati personali relativi alle caratteristiche genetiche ed ereditarie, che forniscono informazioni univoche sulla fisiologia e sulla salute di una persona fisica
  - **Biometrici,** dati personali ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche e comportamentali di una persona fisica
  - **Relativi alla salute,** dati relativi alla salute fisica o mentale di una persona fisica
  - **Altro** (dati personali che rivelano l'origine razziale, etnica, opinioni politiche, convinzioni religiose o filosofiche, ad appartenenza sindacale, dati relativi a vita od orientamento sessuale della persona)
- **Relativi a condanni e reati**

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento ad un identificativo come nome, numero di identificazione, dati relativi ad ubicazione, o più elementi caratteristici della sua identità fisica, fisiologica, genetica, economica, culturale, sociale

DATI (rientranti in categorie) PARTICOLARI*: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

DATI RELATIVI A CONDANNE PENALI E REATI: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, ed applicati a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione, la cancellazione o la distruzione.

TRATTAMENTO DOMESTICO: Il presente regolamento non si applica al trattamento di dati personali effettuato da persone fisiche nell'ambito di attività a carattere esclusivamente personale o domestico. Scopi personali, che non rientrano nelle casistiche, num. telefono, telecamera.

PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica

PSEUDO ANONIMIZZAZIONE: Dati pseudo anonimi non sono considerati propriamente come dati anonimi. Il GDPR non si applica a dati anonimi.

Leggere il Considerando 26 che dici in quali casi si applicano i principi di protezione dei dati e come vengono trattati i dati pseudo anonimizzati.

*Non è permesso trattare dati particolari senza consenso dell'interessato

CONSENSO DELL'INTERESSATO: qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale si manifesta il proprio assenso o consenso, mediante dichiarazioni o azioni.

VIOLAZIONE DEI DATI PERSONALI: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

NORME VINCOLANTI D'IMPRESA: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

CHI TRATTA I DATI PERSONALI?

INTERESSATO: colui al quale si riferiscono i dati che vengono trattati

TITOLARE DEL TRATTAMENTO: è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sulle finalità e sui mezzi di trattamento dei dati personali.

RESPONSABILE DELTRATTAMENTO: è la persona fisica o giuridica alla quale è richiesto di trattare i dati per conto del titolare del trattamento. Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, designare un altro soggetto c.d. *"sub-responsabile"*

INCARICATO: Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se **non è istruito** dal titolare.

DESTINATARIO: La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari.

TERZO: La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

ART 5, I 6 PPRINCIPI DELLA PROTEZIONE DEI DATI

I dati personali sono:

1. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, per fare ciò è necessario fornire un'informativa **(liceità, correttezza, trasparenza**)
2. Raccolti per finalità determinate, e successivamente trattati in modo che non sia incompatibile con le finalità (**Limitazione della finalità**)
3. Adeguati, pertinenti e limitati per quanto riguarda le finalità, si elaborano solo i dati necessari al raggiungimento delle finalità (**minimizzazione dei dati**)
4. Esatti e se necessario aggiornati, devono essere adottate le misure per cancellare o modificare tempestivamente (**Esattezza**)
5. Conservati in una forma che ne permetta l'identificazione per un arco di tempo non superiore al conseguimento delle finalità (**Limitazione della conservazione**)
6. Trattati con adeguata sicurezza, compresa protezione da trattamenti non autorizzati ed illeciti, perdita, distruzione o danno accidentale (**Integrità e riservatezza**)

Il titolare del trattamento deve decidere e dimostrare le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni e specifiche del regolamento (**principio di Accountability**)

IL CONTRATTO

Il contratto è il principale negozio giuridico bilaterale e si definisce come "L'accordo tra due o più parti per costituire, regolare o estinguere un rapporto giuridico patrimoniale", manifestazione di volontà delle parti.

Il contratto a nomina di un responsabile deve riportare la materia disciplinata, natura e finalità del trattamento, tipo di dati trattati e categorie di interessati, obblighi e diritti del titolare del trattamento.

Si può sostituire una manifestazione di consenso con un contratto.

I requisiti del contratto sono:

- **Accordo**, Proposta + accettazione
- **Volontà**, perché sia valida deve essere percepita come espressa o tacita, è rilevante sotto il profilo dell'annullabilità
- **Causa**, funzione socio-economica del contratto, da tipico/atipico
- **Oggetto**, il bene che forma l'oggetto della prestazione contrattuale
- **Forma**, generalmente scritta, le condizioni generali devono esserlo.

Le principali clausole di risoluzione dei contratti sono:

- **Clausola risolutiva espressa,** risoluzione del contratto nel caso in cui non siano adempiute nelle modalità stabilite alcune obbligazioni.
- **Solve et repete,** le parti non possono porre eccezioni al contratto

Contratti ad oggetto informatico si dividono principalmente in:

- **Contratti informatici**, conclusi tramite strumenti informatici
- **Contratti di informatica**, consulenza o servizi
- **Contratti ad oggetto informatico**, aventi SW, HW, sistemi e servizi

ART 6, LICEITA' DEL TRATTAMENTO

Il trattamento è lecito solo se e ricorre almeno una delle condizioni:

a) L'interessato ha espresso il suo **consenso** al trattamento per una o più specifiche finalità
b) Il trattamento è necessario all'esecuzione di un **contratto**
c) Il trattamento è necessario per adempiere ad un **obbligo legale** al quale è soggetto il titolare.
d) Il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica
e) Il trattamento è necessario per **esecuzione di compiti di interesse pubblico**
f) Il trattamento è necessario per il conseguimento del **legittimo interesse del titolare o di terzi**, a condizione che prevalgano i diritti e le libertà fondamentali dell'interessato

ART 9, TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla vita sessuale o orientamento sessuale della persona.

Questo **non** si applica se si verifica uno dei seguenti casi:

a) L'interessato ha prestato il suo consenso
b) Il trattamento è necessario per assolvere ad obblighi e diritti del titolare ed interessato in materia di diritto del lavoro e sicurezza.
c) Il trattamento è necessario per tutelare l'interesse vitale dell'interessato o di un'altra persona fisica
d) Il trattamento è effettuato da fondazioni, associazioni senza scopo di lucro o finalità altre, a condizione che ne riguardino i membri.
e) Il trattamento è necessario in sede giudiziaria

ART 10, TRATTAMENTO RELATIVO A CONDANNE O REATI PENALI

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

ART 12, MODALITA' D'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative ad art 13 e 14, e la comunicazione agli art 15 e 22, relative al trattamento in forma concisa, trasparente e facilmente accessibile.

Le informazioni sono fornite per iscritto o se previsto con mezzi elettronici, oralmente se richiesto dall'interessato.

Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato, non si può rifiutare dal soddisfare una richiesta di un interessato, a meno che non sia in grado di identificarlo, fornisce all'interessato le informazioni relative ad una sua richiesta ai sensi di art 15 e 22, senza ingiustificato ritardo, ed al più tardi entro un mese dalla richiesta.

Se non ottempera alla richiesta da parte dell'interessato, il titolare deve informare entro un mese lo stesso motivandone il perché del rifiuto.

Se le richieste dell'interessato sono infondate o eccessive, il titolare può addebitare delle spese extra, oppure rifiutare di soddisfare la richiesta.

L'INFORMATIVA, spiegazione

Qualora il trattamento sia basato sul consenso, il titolare del **trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.**

L'informativa è una comunicazione rivolta all'interessato con lo scopo di informare sulle finalità e sulle modalità dei trattamenti che fa il titolare. Se il titolare fornisce l'informativa, riesce a provare che assicura trasparenza e correttezza nei trattamenti fin da quando ha progettato il singolo trattamento.

ART 13, INFORMAZIONI DA FORNIRE QUALORA I DATI SIANO RACCOLTI PRESSO L'INTERESSATO – INFORMATIVA 1

In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, l'informativa, questa deve contenere (par 1):

a) Identità e dati di contatto del titolare del trattamento
b) I dati di contatto del responsabile della protezione dei dati

c) Le finalità del trattamento, e la base giuridica
d) I legittimi interessi perseguiti dal titolare o da terzi
e) Eventuali destinatari o categorie di destinatari dei dati personali
f) Ove applicabile, l'intenzione del titolare di trasferire dati personali a un paese terzo o a un'organizzazione internazionale.

In aggiunta a queste informazioni, il titolare fornisce all'interessato ulteriori informazioni relative a periodo di conservazione ed esistenza dei diritti dell'interessato (par 2).

Qualora il trattamento sia basato sul consenso, il titolare del deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso

L'informativa è una comunicazione rivolta all'interessato con lo scopo di informare sulle finalità e sulle modalità dei trattamenti che fa il titolare. Se il titolare fornisce l'informativa, riesce a dimostrate di aver assicura trasparenza e correttezza nel trattamento.

ART 14, INFORMAZIONI DA FORNIRE QUALORA I DATI NON SIANO RACCOLTI PRESSO L'INTERESSATO – INFORMATIVA 2

Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:

Stesse informazioni derivanti dall'art 13, par 1 e 2.

ART 15, DIRITTI DI ACCESSO DELL'INTERESSATO

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) Le finalità del trattamento
b) Le categorie di dati personali in questione
c) Destinatari a cui le informazioni verranno comunicate

d) Quando possibile, il periodo di conservazione
e) L'esistenza del diritto dell'interessato di richiedere al titolare del trattamento la rettifica, cancellazione dei dati, limitazione del trattamento o opposizione.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

ART 16, DIRITTO DI RETTIFICA

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica / aggiornamento / minimizzazione dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

ART 17, DIRITTO ALLA CANCELLAZIONE / OBLIO

L'interessato ha il diritto di richiedere ed ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. Questo nel caso di ritiro del consenso, incompatibilità con le finalità, obblighi legali e trattamenti illeciti.

Il titolare adotta misure ragionevoli, anche tecniche, per informare tutti i possibili altri titolari di cancellare qualsiasi link, copia o riproduzione.

ART 18, DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

L'interessato ha il diritto di ottenere dal titolare del trattamento la sua limitazione nel caso in cui ricorrano alcune casistiche:

a) Viene contestata l'esattezza dei dati
b) Il trattamento è lecito e l'interessato si oppone alla cancellazione e si richiede invece un limite sull'utilizzo

c) Se il titolare non ne ha più bisogno ai fini del trattamento, ma i dati sono necessari all'interessato per accertamento, esercizio o difesa di un diritto in sede giudiziaria.

Se il trattamento è limitato, i dati vengono trattati, salvo conservazione, solo con il consenso dell'interessato.

ART 20, DIRITTO ALLA PORTABILITA'

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare che li ha forniti nel caso in cui:

a) Il trattamento si basi sul consenso ai sensi dell'art 6, o su di un contratto
b) Il trattamento sia effettuato con mezzi automatici

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta da un altro titolare, se tecnicamente possibile.

ART 21, DIRITTO DI OPPOSIZIONE

L'interessato ha il diritto di opporsi in qualsiasi momento per motivi alla situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni.

Qualora i dati siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano per tali finalità, compresa la profilazione.

ART 22, PROCESSO DECISIONALE AUTOMATIZZATO / PROFILAZIONE

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

a) Sia necessaria per la conclusione o l'esecuzione di un contratto tra interessato e titolare
b) Si basi sul consenso esplicito dell'interessato

ART 24, RESPONSABILITA' DEL TITOLARE DEL TRATTAMENTO / ACCOUNTABILITY

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.

Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare.

ART 25, PROTEZIONE DATI AL FINE DI PROGETTAZIONE / MINIMIZZAZIONE

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

ART 26, CONTITOLARI DEL TRATTAMENTO

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni

ART 28, RESPONSABILE DEL TRATTAMENTO

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il **responsabile del trattamento** ("data processor") nel GDPR è definito all'art. 4, par. 1, n. 8) come "la persona fisica, giuridica, PA o ente che elabora i dati personali per conto del titolare del trattamento"

La nomina a responsabile avviene tramite un "contratto di nomina"

ART 29, TRATTAMENTO SOTTO AUTORITA' DI TITOLARE O RSPONSABILE

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ART 30, REGISTRO DEI TRATTAMENTI / ATTIVITA'

Contiene nomi e dati di contatto del titolare del trattamento, del responsabile del trattamento, ed i termini ultimi per la cancellazione.

Contiene le finalità del trattamento, descrizione delle categorie di interessati e delle categorie di dati personali.

Contiene le categorie di destinatari a cui i dati personali sono comunicati, compresi i destinatari di paesi terzi ed organizzazioni internazionali.

ART 32, SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché 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, (anche per quanto concerne il rischio di data breach) che comprendono:

a) Pseudoanonimizzazione e cifratura dei dati
b) Capacità di assicurare su base permanente Confidenzialità, Integrità e Disponibilità dei dati
c) Capacità di ripristinare la disponibilità in caso di incidente
d) Procedure per testare, verificare e valutare l'efficacia delle misure.

ART 33, NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Questo a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve contenere almeno:

a) Descrizione della natura della violazione
b) Comunicare i dati di contatto del responsabile del trattamento
c) Descrivere le possibili conseguenze della violazione di dati personali
d) Descrivere le misure adottate per porre rimedio alla violazione

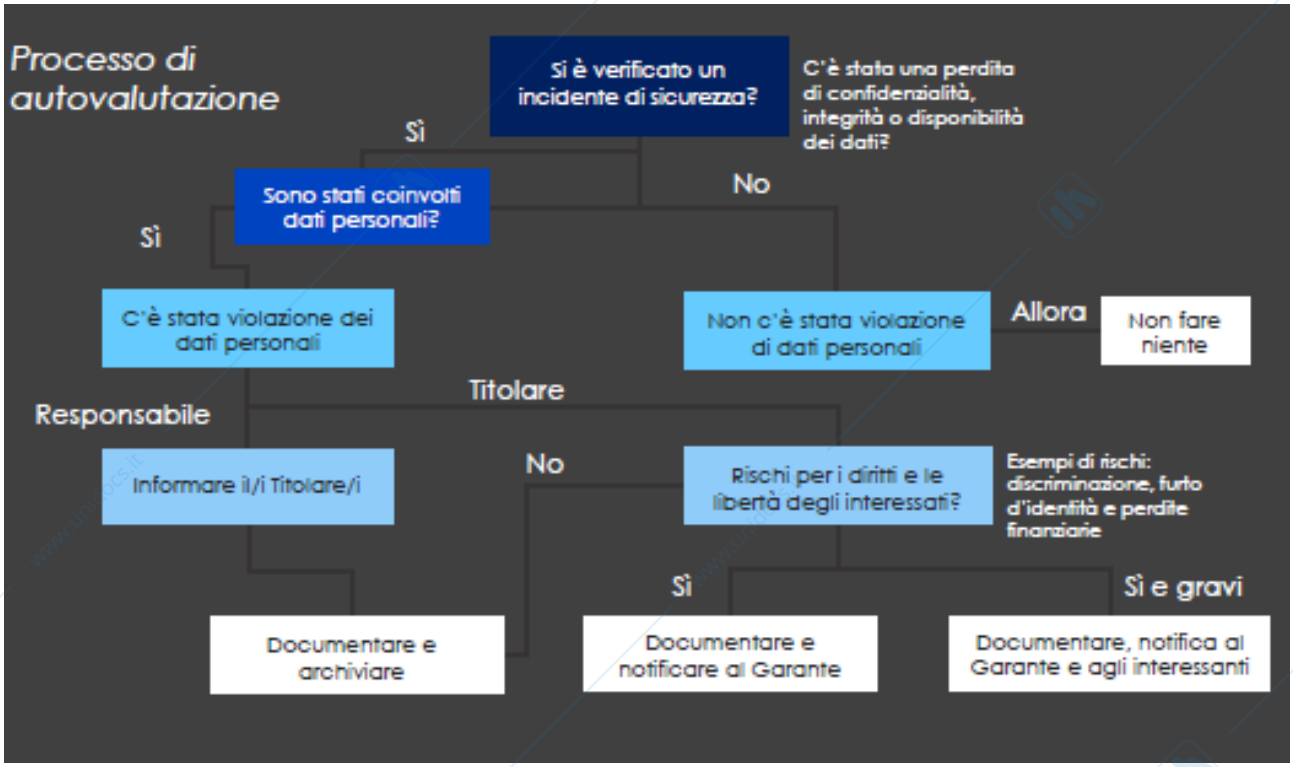
Qualora e nella misura in cui sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite successivamente mediante nota integrativa.

ART 34, COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) Il titolare ha messo in atto misure di sicurezza tecniche ed organizzative adeguate di protezione e tali misure erano applicate ai dati personali oggetto della violazione.
b) Il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà fondamentali degli individui
c) Detta comunicazione richiederebbe sforzi sproporzionati, in tal caso si procede invece con una comunicazione pubblica per informare gli interessati.



ART 35, VALUTAZIONE D'IMPATTO / DPIA

Quando un tipo di trattamento prevede l'uso di nuove tecnologie, e può presentare un livello di rischio, inteso come rischio per i diritti e libertà degli interessati, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali. Presumo che la tecnologia porti danno.

La valutazione contiene almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità
- Una valutazione delle necessità e proporzionalità dei trattamenti
- Una valutazione dei rischi per i diritti e le libertà degli interessati
- Le misure previste per affrontare i rischi

La DPIA è richiesta in particolare nei seguenti casi:

a) Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione

b) Un trattamento su larga scala, di categorie relative a condanne penali o reati
c) La sorveglianza sistematica su larga scala di zone accessibili al pubblico

ART 36, CONSULTAZIONE PREVENTIVA

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Se ritiene che il trattamento previsto violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento

ART 37, DESIGNAZIONE DI UN DPO (DATA PROTECTION OFFICER)

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione nei seguenti casi:

a) Il trattamento è effettuato da un'autorità pubblica
b) Le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala
c) Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10

Larga scala: secondo indicazioni del WP29 numero di soggetti, volume di dati, durata del trattamento, portata geografica.

Regolare: avviene in modo continuo/ ad intervalli regolari / ad intervalli periodici

Sistematica: avviene per sistema, predeterminato, organizzato e metodico, che ha luogo nell'ambito della raccolta di dati

Il **DPO** è un organo di vigilanza e controllo, punto di contatto tra interessato e società, o garante della privacy. E' un soggetto indipendente, P.iva o dirigente con contratto molto particolare, e non può essere penalizzato nella sua condotta, parla con il Board ed il CDA. Viene coinvolto in ogni questione che riguarda la protezione dei dati personali e realizza valutazioni d'impatto sulla protezione de dati (DPIA)

ART 38, POSIZIONE DEL DPO

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia sempre coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39, fornendo risorse necessarie per assolvere tali compiti e accedere ai dati personali e trattamenti.

Gli interessati possono contattare il DPO per tutte le questioni relative al trattamento dei loro dati personali ed esercizio dei loro diritti.

ART 39, COMPITI DEL DPO

Il responsabile della protezione dei dati è incaricato dei seguenti compiti:

a) Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi del regolamento
b) Sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione relative alla protezione dei dati
c) Fornire parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento
d) Cooperare con l'autorità di controllo
e) Fungere da punto di contatto con le autorità

Nell'eseguire i propri compiti, tiene conto dei rischi che il trattamento potrebbe portare ai diritti e le libertà degli interessati.

ART 44, PRINCIPIO GENERALE PER IL TRASFERIMENTO

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale (compresi trasferimenti successivi di dati personali da un paese terzo o altra organizzazione internazionale), **ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo V**, fatte salve altre disposizioni regolamento.

ART 45, TRASFERIMENTO SULLA BASE DI DECISIONI DI ADEGUATEZZA

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

La Commissione Europea può definire delle **delibere di adeguatezza**, con le quali sancisce che un certo paese ha un livello di sicurezza pari a quello dei paesi UE e quindi si possa permettere il trasferimento dei dati. Per concedere la delibera deve prendere in considerazione diversi aspetti come lo stato di diritto, la presenza di autorità di controllo, strumenti giuridicamente vincolanti attivi.

(Evito trasferimenti successivi secondari ed insicuri dei dati tra stati).

Italia e Stati Uniti non hanno accordi di adeguatezza al momento.

La commissione può deliberare una decisione di adeguatezza, si richiede:

- Una proposta della Commissione europea;
- Un parere del comitato europeo per la protezione dei dati;
- Un'approvazione da parte dei rappresentanti dei paesi dell'UE;
- L'adozione della decisione da parte della Commissione europea.

ART 46, 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. Clausole contrattuali tipo da inserire nei contratti per esportare dati.

ART 47, NORME VINCOLANTI D'IMPRESA

L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:

a) Siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o di imprese che svolgono un'attività economica comune
b) Conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali

In assenza di norme vincolanti, si possono utilizzare **delle clausole contrattuali tipo all'interno dei contratti** tra aziende per il trasferimento di dati evitando problematiche a livello di GDPR.

ART 48, TRASFERIMENTO O COMUNICAZIONE NON AUTORIZZATI DAL DIRITTO UE

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, come un trattato di mutua assistenza giudiziaria.

ART 49, DEROGHE IN SPECIFICHE SITUAZIONI

In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

Consenso dell'interessato, Trasferimento per esecuzione di contratto, Motivi di interesse pubblico, Esercitare un diritto in sede giudiziaria, Tutelare interessi vitali dell'interessato, Clausole contrattuali tipo, Norme vincolanti d'impresa.

IL CASO SCHREMS, Privacy Shield

La Corte di giustizia dell'Unione europea (CGUE) si è pronunciata (c.d. "**Sentenza Schrems II**") in merito al regime di trasferimento dei dati tra l'Unione europea e gli Stati Uniti **invalidando la decisione di adeguatezza del "Privacy Shield"**, adottata nel 2016 dalla Commissione europea in seguito alla decadenza del precedente regime di adeguatezza denominato "**Safe Harbor**".

Nella stessa sentenza la CGUE ha inoltre ritenuta valida la decisione 2010/87 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi.

In Europa il trattamento di massa richiede il consenso degli interessati, negli Stati Uniti non si richiede il consenso, ma si deve dimostrare la finalità del trattamento.

Shrems I è stata la prima sentenza che ha stabilito espressamente che le garanzie espresse dalla UE non si limitassero solo all'UE, facendo decadere il "safe arbour", ma deve andare oltre, Il dato nasce e muore con quelle garanzie e lo devono seguire.

Dopo l'invalidità dell'approdo sicuro, il quadro normativo è rimasto scoperto, il trasferimento è avvenuto sulla base di clausole contrattuali tipo di protezione dei dati (Testo standard emanato da commissione nel 2010 su cui si può negoziare).

In seguito entra in vigore lo "Privacy Shield" (Privacy Shield), che rimane valido fino al 2020.

Shrems II fa notare che c'è un comportamento non conforme da parte delle unità americane di Intelligence, che seguono leggi federali, senza seguire alcuni principi come minimizzazione e adeguatezza.

Per il GDPR, la clausola contrattuale può andare a sostituire la decisione di adeguatezza in caso di mancanza

La Corte ha dichiarato invalida la decisione relativa al Privacy Shield, dovuta alle limitazioni alla protezione dei dati personali derivanti dalle leggi statunitensi sull'accesso e utilizzo di questi dati da parte delle autorità pubbliche, oltre che all'assenza di rimedi giudiziali che presentino effettive garanzie per i diritti dei cittadini

ART 50, COOPERAZIONEINTERNAZIONALE PER LA PROTEZIONE DEI DATI PERSONALI

In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per sviluppare meccanismi di cooperazione per facilitare l'applicazione della legislazione sulla protezione dei dati personali, promuovere lo scambio di documentazione e prassi in materia di protezione dei dati personali.

ART 68, COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Il comitato europeo per la protezione dei dati (comitato) è istituito quale organismo dell'unione ed è dotato di personalità giuridica.

Il comitato è rappresentato dal suo presidente

Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno stato membro e dal garante europeo per la protezione dei dati, o dai rispettivi rappresentanti.

ART 83, CONDIZIONI GENERALI PER INFLIGGERE ANZIONI AMMINISTRATIVE PECUNIARIE

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) La natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento
b) Il carattere doloso o colposo della violazione
c) Le misure adottate dal titolare o dal responsabile per attenuare il danno subito dagli interessati.
d) Il grado di responsabilità del titolare o del responsabile tenendo conto delle misure tecniche ed organizzative da essi messe in atto
e) Eventuali precedenti violazioni commesse da titolare e responsabile
f) Le categorie di dati interessate dalla violazione

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, si va dal 2 % del fatturato totale annuo dell'esercizio precedente, fino ad un massimo del 4% per le imprese.

TEMI PRATICI TRATTATI A LEZIONE

Social Spam

1) Siete contattati con un In-box su Facebook, il gestore della pagina della Coca Cola sulla quale hai messo like vi invita ad acquistare un prodotto.

Soluzione: Non si può perché dipende da come interpreto il like, se come consenso o no, non centrano le condizioni.

2) Siete contattati con un In-box su Linkedin, il gestore della pagina della Coca Cola sulla quale hai messo like vi invita ad acquistare un prodotto.

Soluzione: Uguale, non centrano le condizioni, argomentare la liceità della richiesta.

3) Siete contattati con un In-box su Facebook, il gestore della pagina della Coca Cola sulla quale hai messo like vi chiede se la pagina gli piace.

Soluzione: Dipende, occorre spostare l'attenzione sul fatto che chiedere se una cosa ti piaccia sia un'attività di marketing o meno.

4) Siete contattati con un In-box su Linkedin, il gestore della pagina della Coca Cola sulla quale hai messo like vi invita ad un evento al Club House.

Soluzione: Dipende, si deve domandarsi se il like esprime un consenso, se seguito da un'informativa inviata dalla pagina di Coca Cola. Se l'evento è del Club House, avrei dovuto dargli il mio consenso, allora non è lecito perché il dato è trattato da un titolare del trattamento senza consenso.

5) Siete contattati con un In-box su Instagram, la supermodella XY ci chiede se eravate voi a ballare sul cubo perché ci vuole conoscere.

Soluzione: Va bene solo se è lei, è trattamento domestico, do consenso.

Caso DPIA

Contesto: Associazione che raccoglie i reclami sulle violazioni dei diritti degli interessati, per segnalare comportamenti illeciti (riguardanti violazioni dei diritti degli interessati) al garante della privacy.

I diritti degli interessati sono i seguenti:

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

Dati raccolti dall'associazione:

- Nome
- Cognome
- Email
- Azienda con cui l'interessato ha avuto problemi

Trattamento:

- Raccolta dei dati elencati in precedenza
- Utilizzo di tali dati al fine di contattare il garante

Valutazione degli impatti in caso di mancanza di:

- Confidenzialità: ALTO
  - Rivelazione dell'associazione tra interessato e azienda con cui ha il problema. Per esempio: se l'interessato lavora per questa azienda, potrebbe subire ripercussioni sul luogo di lavoro/sulla carriera/sulla vita privata
- Integrità: ALTO
  - Nel caso di alterazioni nei dati si possono avere azioni intraprese contro aziende che non erano presenti nei dati. Per esempio: viene alterato il nome di una azienda dal database con quello di un'altra azienda estranea ai fatti

Data Breach

Prima domanda da farsi per sapere se è in corso un data Breach:

E' avvenuto un incidente di sicurezza che ha coinvolto una perdita di una delle tre proprietà CIA? La notifica di violazione dell'autorità di controllo deve avvenire entro 72 ore. Il responsabile informa il titolare senza ingiustificato ritardo.

La notifica può essere:

- Completa, se so già tutto e posso comunicarlo
- Preliminare, inizio con una comunicazione senza troppe informazioni e poi ne fornisco una completa in un secondo momento (notifica integrativa)

Seguendo l'art 34 (Per violazioni gravi): il titolare del trattamento o il suo DPO fanno una valutazione di impatto e riscontrano un possibile rischio per i diritti e le libertà, allora provvedono a notificare l'interessato.

Una violazione può essere gestita definendo e seguendo policy.

E' il titolare che valuta la gravità della situazione, decide se notificare il garante e/o l'interessato.

Caso Data Breach, attacco Ramsomware

Sicuramente è in corso un data breach, è venuta meno la disponibilità dei dati, molto probabilmente anche la confidenzialità.

Chi ha lanciato l'attacco possiede una copia dei dati (può avere capacità di divulgazione)

- Consultiamo il piano di Incident-Response aziendale
- Controlliamo lo stato generale del sistema, quali macchine sono state colpite, se i backup sono integri o meno
- Cerchiamo di capire il punto d'ingresso in rete del virus
- Sviluppiamo un piano di contenimento
- Mettiamo in atto azioni di eradication e remediation
- Fast recovery, businness continuity e disaster recovery

Caso sul trasferimento

Casa farmaceutica italiana (multinazionale) che per un servizio di marketing deve trattare dei dati e le altre del gruppo sono in Francia Svizzera Regno Unito e Stati Uniti.

Tutte raccolgono dati in maniera differente e quindi devono riuscire ad aggregarli. E solo la capogruppo italiana spedirà la newsletter. Quali misure sono adeguate al trattamento a norma del GDPR?

Dire che genere di dati tratta → dati particolari.

Dire quali misure relative al trasferimento deve porre in essere ai fini del trasferimento. → Art 46 e 47, abbiamo un problema relativo alle decisioni di adeguatezza da considerare per Svizzera e Regno Unito, No Stati Uniti.

Sei dati viaggiano da US verso Europa non abbiamo problemi perché sono tutti compliant al GDPR. Al contrario se viaggiano da Europa verso Estero, se non ci sono deroghe applichiamo le clausole standard del 46.

Caso 1, l'esportazione

La Superpenn S.r.l si occupa di verifica della sicurezza di software. Per svolgere le proprie attività delega alcuni test alla Cesano lt. Società di Singapore, la quale deve poter disporre dei software e dei DB che stanno alla base dei software stessi. I tempi sono brevi. L'analisi avviene in territorio di Singapore. Nessun interessato ha mai reso consenso all'esportazione. Come può la Superpenn s.r.l. esportare dati personali?

- Uso di clausole contrattuali tipo, che sono però dei contratti che devono essere approvati. Devo firmare una nomina a responsabile.

Uso dell'articolo 49, utilizziamo una deroga perché c'era già un contratto in essere, in quanto non è possibile applicare il 45 o 46 perché Singapore non è sotto decisione di adeguatezza.

Caso 2, Le email

Lo store online della nota casa di abbigliamento GOODLIFE è gestito mediante contratto di full-outsourcing, da "La Faina S.r.l.". La Goodlife vorrebbe potere inviare ai clienti che hanno acquistato sul proprio sito i prodotti, delle email a scopo promozionale. E' possibile identificare una soluzione, che implichi un numero particolarmente basso di consensi (flag box di espressione di consensi) al fine di aumentare le conversioni (accesso convertito in un acquisto/fatturazione)?

Dare un incentivo, se mi iscrivo ad una newsletter ho lo sconto, ma il consenso non è liberamente prestato.

Il problema è relativo a chi è che stipola il contratto, tutto viene fatto da La faina, ma lo vorrebbe fare Goodlife.

Se ho un contratto di full out sourcing, Goodlife stipula il contratto con faina, se il contratto scade non è possibile trasferire i dati senza problemi.

La faina è titolare del trattamento, può fare un contratto di nomina a responsabile con Goodlife.

Sul sito gestito da faina ci sarà l'informativa da parte di faina.

Quando c'è il carrello metto un flag che presta il consenso alla Goodlife, fornendo un'altra informativa per contratto con finalità di marketing ma questa volta a favore di Goodlife e non più a la faina.

Caso 3, Stargate

Due società ortopediche vengono acquistate da una holding controllante, che mette a disposizione loro la medesima piattaforma Cloud gestionale. Entrambe le società iniziano a lavorare con i marchi della holding, ed hanno intenzione di offrire un servizio tale per cui ciascun paziente può essere visitato in entrambe le cliniche. E' evidente tuttavia che per una visita medica i dati pregressi del paziente debbano essere in possesso della clinica che effettua la visita. Se il paziente si è fatto visitare nella

società A e decide di farsi visitare in B, B dovrebbe disporre del pregresso medico. Come può questo avvenire lecitamente?

Essendo due titolari del trattamento occorre un contratto di contitolarità tra le due società su dati di natura particolare, secondo l'articolo 26. Sta in piedi ma dobbiamo evitare i contratti di contitolarità come il demonio.

Ci si appella al diritto alla portabilità, prevedo un modulo tale per cui, una persona firma per la portabilità dei dati quando si presenta in clinica (interoperabilità del dato in sede di Cloud condiviso). A e B si accordano in maniera tale da trasferire i dati di A verso B e viceversa previa firma.

Caso 3, Cinque euro, due cookie

La Alongi spa, vuole utilizzare GA4 per avere statistiche relative al proprio sito web, vetrina dei prodotti... ma può?

La risosta è dipende, il garante italiano dice, in particolar modo se tu sei loggato con Google, loro possono incrociare i tuoi dati. Se non sei loggato, hai anonimizzato IP, disattivi Google signal, inizia a mettere marcatori pagina per pagina, dividi unificazione delle sezioni, no mixing cookie, se adotto tutti questi tipi di misure potrebbe essere lecito ma non si sa.

Se riesco ad arrivare ad un livello di anonimizzazione fortissimo poi GA4 non gira bene e perdo troppe info. Si sta aspettando un nuovo Privacy Shield che permetta il trasferimento sicuro dei dati.

Caso 4, A Dubai c'è tutto

A Dubai c'è veramente di tutto, ho guadagnato 2 milioni di euro facendo drop shipping da casa, mettendo in affitto immobili a Pozzuoli, senza possederli, affittati a 200 euro al mese in affitto a 1500.

Vivo a Dubai da qualche anno, le mie consulenze costano 90k all'ora, vivo in un attico da 2500 metri quadri e cambio una macchina al mese. Dopo aver promosso il corso, vengo condannato per truffa ed evasione fiscale da un tribunale italiano.

Decade qualche anno dalla condanna e espiata la sanzione, Si chiede a Google di deindicizzare dal proprio motore di ricerca gli articoli relativi alla condanna. Google decide di rispondere affermativamente ma solo dalla versione italiana.

Una volta giunto a Dubai si nota che il nome è ancora presente anche nelle versioni locali del motore di ricerca. E' possibile richiedere a Google la deindicizzazione anche sulla versione locale?

Da sentenza CNIL da corte di cassazione, l'autorità italiana può decidere di imporre all'autorità di controllo di richiedere la cancellazione e deindicizzazione globale. (Vedi sentenza cassazione Dicembre 2022)

Caso 5, nei miei sogni sono così

Simone Bonavista e Valentina Vitkovenko hanno un figlio e dopo qualche mese si separano. Marco a 16 anni diventa testimonial di uno stilista e sottoscrive un accordo di cessione dei propri diritti di immagine a titolo gratuito. Ritenendo che è un Brand Valentina vorrebbe monetizzare.

Simone trasferitosi in Svezia, viene a conoscenza della questione ed intendendo monetizzare l'immagine del figlio si rivolge a voi, consulenti di privacy, per raccogliere suggerimenti.

Avrei potuto chiedere il consenso ad utilizzare le immagini. Lato privacy è difficile attaccare un minore che firma, la madre è a favore del contratto.

Abbiamo un contratto che comporta il consenso di Marco ed uno dei due genitori. Il potere di firma sarebbe di entrambi i genitori.

Avrebbero dovuto essere firmati da entrambi i genitori per art 320 cc oppure essendo un atto che va a dare compensi al figlio, avrebbe dovuto esserci necessità di passare da un giudice.

PROVVEDIMENTI DEL GARANTE

VIDEOSORVEGLIANZA, 8 aprile 2010

Raccolta, registrazione, conservazione, in generale l'utilizzo di immagini configura un trattamento di dati personali (Art 4)

E' considerato dato personale, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Condizioni di liceità per la videosorveglianza:

1. **Protezione e incolumità** degli individui, relativi alla sicurezza urbana e/o pubblica, prevenzione, accertamento o repressione di reati.
2. **Protezione della proprietà, atti vandalici**
3. **Rilevazione, prevenzione e controllo infrazioni di soggetti pubblici**
4. **Acquisizione di prove**

Deve rispettare il principio di proporzionalità, liceità, il principio di privilegio minimo per il responsabile, il Garante dà indicazioni di massima.

Il GDPR non si applica (trattamento dati personali) in ambito domestico.

La videosorveglianza deve rispettare il codice Privacy, lo Statuto dei lavoratori, il divieto di interferenza illecita nella vita privata, in materia di sicurezza negli impianti sportivi, porti, stazioni e linee di trasporto.

Principi che la pratica della videosorveglianza deve rispettare:

- Liceità del trattamento, bilanciamento degli interessi
- Principio di necessità (e minimizzazione)
- Proporzionalità
- Valutazione d'impatto (art. 35 GDPR)
- Misure di sicurezza
- Nomina dei responsabili
- Informativa (Minima ed estesa)

POSTA ELETTRONICA ED INTERNET

Nello specifico, segnalazioni e reclami pervenute riguardo i trattamenti di dati personali effettuati da datori di lavoro mediante l'uso di strumenti informatici e telematici.

Riguardo la posta elettronica e rete internet nel rapporto di lavoro:

- Compete al datore di lavoro assicurare la funzionalità di tali mezzi da parte dei lavoratori, definendone le modalità d'uso, tramite una policy ben chiara ed aggiornata
- Spetta a lui essi adottare misure di sicurezza idonee per assicurare integrità, disponibilità di dati e prevenire accessi indebiti
- L'analisi dei Log da parte del titolare può essere fatta rispettando i principi di trasparenza, limitazione delle finalità, minimizzazione, integrità e riservatezza
- I servizi di posta sono parametri suscettibili di controlli che possono giungere alla conoscenza del contenuto da parte del datore di lavoro, tuttavia ne è vietata la lettura diretta.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati, il principio di necessità (riduco al minimo l'utilizzo di dati personali) e principio di correttezza (finalità trattamento note ai lavoratori).

All'onere di definire una policy, si affianca il dovere di informare gli interessati ai sensi dell'Art. 13 con un'informativa con le principali caratteristiche dei trattamenti ed i diritti degli interessati.

Non è ritenuto lecito il trattamento effettuato mediante strumenti HW e SW (controllo a distanza) grazie alle quali si può ricostruire l'attività del lavoratore.

Il datore di lavoro può avvalersi legittimamente di sistemi che permettono un controllo a distanza indiretto per un trattamento dei dati personali dei lavoratori per esigenze produttive, organizzative o di sicurezza sul lavoro. Il trattamento che ne segue può risultare illecito.

I sistemi SW e HW devono essere configurati in modo da cancellare periodicamente i dati personali relativi ad accessi internet e traffico la cui conservazione non sia necessaria.

AMMINISTATORE DI SISTEMA

Questa figura professionale si dedica alla gestione e manutenzione di sistemi di elaborazione con cui si effettuano trattamenti di dati personali.

Compresi i sistemi di gestione delle basi di dati, sistemi software complessi come ERP, reti locali ed apparati di sicurezza, nella misura in cui si consente di intervenire sui dati personali.

Secondo il Garante, durante la nomina di un'Ads, è utile per il titolare:

- Valutazione delle caratteristiche soggettive
- Designazioni individuali ed ambiti di operatività
- Elenco degli Ads presenti e funzioni attribuite
- Elenco di eventuali Ads in outsourcing
- Verifica periodica (annuale) dell'operato
- Adottare sistemi idonei alla registrazione degli accessi

MARKETING E PROFILAZIONE

Secondo La richiesta di Ferragamo di verifica preliminare in ambito "Fidelity Card" e garanzie dei consumatori (programmi di fidelizzazione):

Tale provvedimento ha stabilito che chiunque voglia conservare i dati della propria clientela per finalità di profilazione e marketing, per un periodo superiore a dodici mesi, deve presentare al Garante una richiesta di verifica preliminare, ai sensi dell'Art. 17. (Diritto di cancellazione/oblio)

Il Garante ritiene che per i dati personali relativi ad acquisti di fascia alta è ragionevole ritenere che dodici mesi siano pochi data la frequenza degli acquisti e proroga la durata a sette anni.

Alla scadenza della durata, i dati devono essere cancellati automaticamente, ovvero resi anonimi in modo permanente.

Bisogna ricordare comunque che il principio fondamentale su cui si basa la tutela dei dati personali è quello dell'informativa, cioè devono sempre essere rese le finalità per i quali i dati sono raccolti e soprattutto il consenso da parte dell'interessato.

Nel caso della profilazione, si dovrà presentare un'informativa agli interessati, che specifica nella parte delle finalità, che il trattamento avviene nel rispetto delle garanzie e delle misure prescritte dal Garante.

L'informativa dovrà inoltre contenere anche l'indicazione delle finalità ulteriori ed eventuali per le quali i dati potranno essere trattati solo qualora l'interessato rilasci uno specifico consenso aggiuntivo per finalità di marketing diretto o automatizzato.

Si ricorda che è solo il titolare a poter svolgere l'attività di marketing.

Qualora si volesse demandare questa ad un altro soggetto terzo, si dovrebbe richiedere agli interessati un ulteriore consenso, relativo alla comunicazione dei dati a terzi. A loro volta i terzi devono acquisire consenso per l'attività promozionale.

COSTUMER CARE IN AMBITO SANITARIO

Nell'ambito del trasferimento di dati da una clinica/ospedale ad un altro.

Si ricorda che le persone hanno diritto alla portabilità dei dati, ossia di riceverli in formato strutturato e leggibile. Questo diritto può essere esercitato solo se i dati personali sono stati raccolti nell'ambito di un contratto o sulla base del consenso e se trattati con mezzi automatizzati.

Essendo due titolari del trattamento, occorre un contratto di contitolarità tra le due società su dati di natura particolare, secondo l'articolo 26.

Si cerca comunque di evitare i contratti di contitolarità come il demonio.

Ci si appella al diritto alla portabilità, prevedendo un modulo tale per cui, una persona firma per la portabilità dei dati quando si presenta in clinica (interoperabilità del dato in sede di Cloud condiviso).

Le cliniche A e B si accordano in maniera tale da trasferire i dati di A verso B e viceversa previa firma di un nuovo contratto tra le parti.

COOKIE

Il considerando 30 del Regolamento afferma che "Le persone fisiche possono essere associate a identificativi online prodotti da dispositivi, applicazioni, strumenti e protocolli come indirizzi Ip, marcatori temporanei o cookie o identificativi di altro tipo".

Tali identificativi, se combinati con altre informazioni ricevute dai server, possono essere usate per re-identificare le persone fisiche.

Come noto, i cookie sono stringhe di testo che i siti web visitati posizionano o archiviano all'interno di un dispositivo terminale.

Nelle linee guida, l'Autorità suddivide i cookie in due macro categorie:

- **Cookie tecnici**: necessari al corretto funzionamento del sito, non necessitano del consenso dell'interessato.
- **Cookie di profilazione**: che raggruppano profili degli utenti in cluster omogenei per permettere di inviare messaggi pubblicitari mirati agli utenti, in linea con le preferenze

Per l'utilizzo di cookie e degli altri identificatori tecnici, il titolare del trattamento deve fornire obbligatoriamente informativa specifica.

I cookie di tracciamento per finalità diverse da quelle tecniche potranno essere utilizzate solo previa acquisizione del consenso, informato.

I cookie di "analytics" usati per misurare il traffico, vengono considerati come tecnici, e come tali possono essere utilizzati in assenza del consenso dell'interessato.

Secondo il Garante, il semplice "scroll down" del cursore della pagina è inadatto a rappresentare una forma di consenso, per il titolare del trattamento, ad installare e utilizzare un cookie di profilazione.

Simile approccio riguarda anche il "Cookie Wall", con il quale l'utente viene obbligato a prestare il consenso alla ricezione e invio di cookie senza alternativa per visitare la pagine web.

PRIVACY BY DESIGN E BY DEFAULT

Il principio di **Privacy by design** è un concetto basato sulla prevenzione dei rischi che si può riassumere in alcuni punti:

- Prevenzione e non correzione di problemi in fase iniziale
- Privacy come impostazione di default
- Privacy incorporata nel progetto aziendale
- Sicurezza dei dati durante tutto il ciclo del servizio o prodotto
- Principio della trasparenza

Il principio di **privacy by default** stabilisce che le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Significa semplicemente che un'azienda non dovrà ricorrere all'utilizzo di eccessivi dati senza motivi specifici.

"ATTIVITA' PROMOZIONALE E CONTRASTO ALLO SPAM"

Riguardo il "marketing mirato", grazie all'uso di meccanismi di profilazione dell'utente ed invio automatizzato, ed il "social spam".

Il Garante ravvisa di seguire le linee guida con le seguenti finalità:

- Tenere conto del quadro normativo mutevole
- Chiarire alcuni profili problematici relativi al social spam
- Inquadrare alcune nuove forme di spam, con l'intento di limitare i rischi connessi alle nuove tecnologie.

Lo Spam è definito come l'insieme di comunicazioni per l'invio di materiale pubblicitario o vendita diretta per il compimento di ricerche di mercato e comunicazione commerciale, effettuate in violazione delle norme, con mezzi automatizzati e senza il consenso dell'interessato.

Mentre le persone fisiche possono esercitare i loro diritti come espresso dall'Art. 7 (condizioni per il consenso), le persone giuridiche non possono.

Alle comunicazioni automatizzate sono applicabili i principi di correttezza, finalità e correttezza del trattamento.

Un imprescindibile obbligo del titolare del trattamento è quello di fornire ai destinatari delle comunicazioni promozionali di un'informativa, adeguata al trattamento dei dati, nonché richiedere il consenso per l'invio di mail per finalità commerciali.

Il consenso del contraente per l´attività promozionale deve intendersi libero quando non è preimpostato e non risulta obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento.

Secondo direttiva, il consenso può essere fornito secondo qualsiasi modalità appropriata che consista all'utente di esprimere liberamente ed in conoscenza di causa i sui desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito internet

Per quanto riguarda le finalità del trattamento, il titolare del trattamento deve acquisire uno specifico consenso per ciascuna diversa finalità, ad esempio: marketing, profilazione comunicazione a terzi.

Per la sola posta elettronica, può ricorrere l'eccezione "Soft Spam" secondo la quale, se il titolare utilizza indirizzi di posta a fini di vendita diretta di propri prodotti o servizi, può non richiedere il consenso. Questo sempre che l'interessato sia informato e non ne rifiuti l'utilizzo.

Il "Social Spam" consiste nell'insieme di attività mediante le quali lo spammer veicola messaggi e link attraverso le reti social online, ed i messaggi promozionali inviati tramite social network (Facebook) sono soggetti ad Art. 3, 11, 13, 23, 130.

Se l'utente riceve un messaggio privato, il trattamento è illecito.

Se l'utente è diventato fan di una pagina o è diventato "follower" di un determinato marchio, personaggio, prodotto, e riceve messaggi pubblicitari, il trattamento può considerarsi lecito perché si considera la volontà di seguire un marchio come manifestazione della volontà di prestare consenso alla ricezione di messaggi.

FIDELITY CARD

Le carte di fedeltà vengono rilasciate anche se il consumatore non intende acconsentire ad eventuali iniziative di profilazione o di marketing.

Quando le informazioni vengono usate anche per costruire profili di consumatori, ricerche di mercato o direct marketing, i consumatori devono esprimere, liberamente e senza sollecitazioni il consenso all'uso.

Le regole rispetto alle fidelity card riguardano le tre principali finalità per i quali i dati vengono trattati:

- La fidelizzazione, che viene realizzata attribuendo vantaggi al cliente
- La profilazione, mediante analisi delle abitudini e scelte di consumo
- Il marketing diretto

Il primo obbligo per chi rilascia una carta fedeltà è quello di informare in maniera chiara e completa sull'uso che verrà fatto dei dati e le finalità.

L'informativa al cliente deve essere resa chiara attraverso moduli di sottoscrizione, per ogni altra finalità di trattamento si necessita di un consenso specifico

Il Garante richiede di trattare i dati seguendo i principi di necessità (minimizzazione), liceità, correttezza, qualità dei dati.

Per quanto riguarda la fidelizzazione, viene stabilito che possono essere trattati senza il consenso solo i dati necessari per attribuire vantaggi.

Per quanto riguarda l'attività di profilazione, occorre il consenso dell'interessato per il trattamento delle informazioni relative agli acquisti.

Riguardo all'attività di marketing diretto, possono essere raccolti ed utilizzati dati necessari e non eccedenti all'invio di materiale pubblicitario o comunicazioni commerciali o per la vendita diretta. L'eventuale utilizzo dei dati personali richiede un consenso specifico da parte dell'interessato.

IL FIGLIO DEL BONAVISTA

Simone Bonavista, ha un conto corrente presso la Banca di Bordighera, con una giacenza di circa 3 milioni di euro. Dopo aver regalato per i sui 18 anni una somma di euro 500.000 alla figlia, mediante un bonifico, chiama in filiale chiedendo all'operatore, come ha sempre fatto, la giacenza del conto della figlia, scoprendo che questa aveva sul conto una somma pari a 30 milioni di euro. La figlia, ricevuta la chiamata dal padre, chiama la banca per chiedere delucidazioni.

Il trattamento in questione risulta illecito in quanto posto in essere in violazione dei principi generali in materia di protezione dei dati personali.

Si ritiene che non è applicabile al caso in questione la Buona fede, la banca non ha rispettato il principio di Accountability e non ha correttamente istruito il personale a rispondere a tale caso.

IL DIPENDENTE DECONCENTRATO

Il dipendente lavora come centralinista presso la vostra azienda. I dirigenti lo sorprendono, più` volte, a visitare siti a carattere pornografico. Numerosi computer vengono infettati da virus dopo aver ricevuto file dal computer del dipendente. L'amministratore vuole licenziarlo. Ha bisogno di prove: il dipendente, infatti ha negato ogni addebito.

Per contestare l'indebito uso di beni aziendali, sarebbe stato sufficiente verificare gli avvenuti accessi e tempi di connessione senza indagare sui contenuti dei siti; La società ha invece operato un trattamento diffuso di informazioni operando in modo eccedente e non trasparente.

I dati personali raccolti potevano essere trattati dal datore di lavoro senza consenso solo se indispensabili per far valere un diritto in sede giudiziaria.

Va rilevato, che non risulta che il dipendente avesse la necessità di accedere ad internet per svolgere il proprio lavoro (Accountability del titolare). Per ciò che ne concerne, il merito va rilevato alla società che non ha fornito un'informativa relativa al trattamento dei dati personali.

E' illecito spiare il contenuto della navigazione in internet del dipendente.

LA PAURA DEL COMPITO DI GRECO

Il preside dell'istituto Beato Bonavista di Trezzano sul Naviglio Ligure, vi convoca. Vostro figlio, venerdì alle ore 13.00, poco prima del termine delle lezioni, è andato in bagno, ha bloccato i rubinetti, ed ha allagato tutto il liceo, lasciandoli aperti per 2gg. Le telecamere, delle quali ignorava l'esistenza, hanno ripreso tutto.

Contesto se le telecamere sono segnalate, se c'è l'informativa, se sono posizionate in bagno o all'esterno, contesto il tempo di conservazione. Giuridicamente parlando la ripresa non potrebbe essere fatta durante l'ora di lezione, circoscrivendo le sole aree soggette a furti e atti vandalici.

Magari il quartiere non è affetto da problematiche di criminalità e quindi la finalità del trattamento non è giustificata, cioè trattamento illegittimo. Servivano le telecamere ove ci doveva essere un bidello a controllare? Si sarebbe dovuto usare il principio di minimizzazione del trattamento.

C'è un vademecum sulla privacy in ambito scolastico (LEGGERE)

DI PINTA

VISTO il reclamo presentato, ai sensi dell'Art. 77 (diritto di porre reclamo all'autorità di controllo) da sig. Bonavista nei confronti della proloco di Bordilandia, con cui l'interessato ha lamentato una violazione della normativa in materia di protezione dei dati personali in relazione alla diffusione sulla pagina Facebook della predetta associazione di due fotografie che ritraggono il reclamante Bonavista, Comandante della polizia locale, durante l'evento Bordilandia Di-Pinta.

Considerato che il reclamante ha dichiarato che gli scatti in area pubblica siano stati fatti e diffusi con scopo denigratorio, nel caso in esame sussiste l'interesse pubblico, il Garante dice che non è denigratorio in quanto ritraeva la persona su luogo di lavoro. Cambia la decisione a seconda del contesto.

Secondo il Garante, I funzionari pubblici e i pubblici ufficiali, comprese le forze di polizia impegnati in operazioni di controllo o presenti in manifestazioni o avvenimenti pubblici, possono essere fotografati e filmati, purché non sia espressamente vietato dall´Autorità pubblica.

L´uso delle immagini e delle riprese deve però rispettare i limiti e le condizioni dettate dal Codice in materia di protezione dei dati personali. Le persone riprese che ritengono lesi i propri diritti possono sempre far ricorso ai rimedi previsti dall´ordinamento sia in sede civile che penale.

LA VISITA MEDICA provvedimento 5 marzo 2020

I signori Bonavista, in qualità di esercenti la potestà del figlio minore, hanno lamentato l'inserimento nel registro elettronico della classe del liceo scientifico di Borghenuovo frequentata dal figlio, di una nota contenente informazioni relative alla salute di quest'ultimo. In particolare, sul registro elettronico sarebbe stato trascritto "con cadenza settimanale nel corso dell'anno 22/23 era soggetto a visita medica".

Il Liceo, riconoscendo l'avvenuta violazione ha provveduto ad oscurare l'annotazione oggetto di contestazione; La segnalazione di eliminazione da parte della famiglia è stata accolta e lavorata in tempi più stretti.

La pubblicazione di tali dati sul registro elettronico non è un'operazione consolidata ma si tratta di un caso isolato e involontario.

Il Garante ha ritenuto illecito il trattamento da parte del Liceo in violazione degli Art. 4, 5, 9 del regolamento in relazione alla pubblicazione sul registro elettronico, accessibile da tutti i genitori, di una nota riguardante informazioni relative alla salute del figlio.

Il FIGLIO STRAVAGANTE

Vostro figlio, un adolescente come tanti va spesso in discoteca ed in giro con gli amici. Un giorno, viene da voi molto preoccupato; qualcuno all'ingresso della discoteca lo ha filmato ed ha messo tutto su internet.

Come per gli mms, le videochiamate o registrazioni possono avvenire o circolare tra persone fisiche per fini esclusivamente privati. In questi casi se non vengono comunicati a terzi, la normativa in materia di protezione dei dati non è applicabile.

Le immagini e suoni ripresi per uso personale potrebbero riguardare terzi ed essere diffusi tramite web, il trattamento dei dati è lecito solo se sono rispettate tutte le disposizioni applicabili dal codice.

Questo comporta il dovere di informare preventivamente l'interessato, di raccogliere il consenso libero, preventivo ed informato e di osservare tutte le altre cautele previste.

STOP ALL'USO DI ANALYTICS

Il sito web che utilizza il servizio Google Analytics (GA) senza le garanzie previste dal regolamento UE, viola la normativa sulla protezione dei dati perché trasferisce negli Stati uniti, paese privo di un adeguato grado di protezione per i dati degli utenti.

Dall'indagine del Garante è emerso che i gestori dei siti web che utilizzano GA raccolgono, mediante cookie, informazioni sulle interazioni degli utenti con i predetti siti, le singole pagine visitate e i servizi proposti.

Tra i molteplici dati raccolti, indirizzo IP del dispositivo dell'utente e informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata, data e ora della visita al sito web.

Tali informazioni sono risultate oggetto di trasferimento verso gli US.

Nel dichiarare l'illiceità del trattamento è stato ribadito che l'indirizzo IP costituisce un dato personale e anche nel caso fosse troncato non diverrebbe un dato anonimo, considerata la capacità di Google di arricchirlo con altri dati di cui è in possesso.

Il Garante ha evidenziato, in particolare, la possibilità, per le Autorità governative e le agenzie di intelligence statunitensi, di accedere ai dati personali trasferiti senza le dovute garanzie.

l'Autorità richiama all'attenzione di tutti i gestori italiani di siti web, pubblici e privati, l'illiceità dei trasferimenti effettuati verso gli Stati Uniti attraverso GA.

SICUREZZA E PRIVACY SENZA ESAGERARE

Con reclamo del XX, una dipendente del Comune di Bolzano ("il reclamante") ha lamentato presunte violazioni della disciplina di protezione di dati personali con riguardo al trattamento di dati posti in essere dall'Ente mediante il monitoraggio del traffico di rete e dei singoli accessi ad Internet effettuati dall'interessato e dai dipendenti comunali.

Con il reclamo è stata lamentata la violazione dei principi di liceità, correttezza e minimizzazione nel trattamento dei dati personali dei dipendenti del Comune, atteso che il sistema di registrazione degli accessi ad Internet impiegato dall'Ente consentirebbe di controllare, tracciare, filtrare la cronologia dei siti internet visitati e il tempo di navigazione di per ciascun sito, nonché la memorizzazione e la conservazione di tali dati associati a ciascun dipendente per un lungo periodo di tempo.

Il Garante rileva che il Comune ha posto in essere trattamenti di dati personali dei dipendenti relativi alla navigazione Internet, anche estranei all'attività lavorativa, in assenza di un idoneo presupposto di liceità del trattamento, di un'idonea informativa, e di una valutazione di impatto sulla protezione dei dati.

Nel rispetto del principio di "liceità, correttezza e trasparenza" il titolare deve adottare misure appropriate per fornire all'interessato tutte le informazioni in forma completa, trasparente e facilmente accessibile.

Il trattamento deve essere "necessario" rispetto alla finalità perseguita ed avere come oggetto i soli dati pertinenti.