Nome Referente Corso: Franco
Cognome Referente Corso: Guenzi

FASTMARKETWEB
CORSO REGOLE E PRINCIPI FONDAMENTALI DEL GDPR

Con il **GDPR** è previsto, per la prima volta a livello normativo, l'obbligo da parte del titolare del trattamento di dimostrare il rispetto della normativa secondo l'importanza, la quantità e la particolarità dei dati che sono trattati in azienda con la possibilità di quest'ultima di intervenire con i giusti correttivi. Il titolare del trattamento deve mettere, quindi, in atto tutte le misure di sicurezza necessarie per garantire un'adeguata protezione dei dati, sia digitali sia cartacei.

Le misure di precauzione devono garantire un **livello di sicurezza adeguato al rischio**.

Qui di seguito proponiamo uno specchietto che illustra le priorità minime di gestione obbligatorie, mentre nella relazione successiva, sono indicate ulteriori condizioni di sicurezza, per le quali vi consigliamo di attuare azioni correttive che vi permetteranno di determinare il massimo requisito di adeguamento alla normativa in vigore.

SPECCHIETTO DELLE PRIORITA' AMBIENTALE E DATI CARTACEI

Legenda O OBBLIGATORIO O CONSIGLIATO O FACOLTATIVO

PRODOTTO	1-2 UTENTI	3-5 UTENTI	5-10 UTENTI	10-20 UTENTI	+ 20 UTENTI
Protezione Dati Cartacei					
Cartelline pseudonimizzate	O	O	O	O	O
Contenitori con chiave	O	O	O	O	O
Armadi con chiave	O	O	O	O	O
Armadi ignifughi	O	O	O	O	O
Formazione del Personale					
Formazione	O	O	O	O	O
Consegna policy	O	O	O	O	O
Consegna incarico e mansionario	O	O	O	O	O
Ambientale					
Video Sorveglianza	O	O	O	O	O
Sistema di Allarme	O	O	O	O	O

Il GDPR UE evidenzia la protezione dei dati personali, compiendola **a partire dal momento dell'ideazione e in modo implicito** (by design and by default). Detto questo, implementare i metodi di sicurezza e protezione dei dati è a discrezione di ogni organizzazione che segua i più recenti e i migliori metodi.

Protezione Dati Digitali

Legenda O OBBLIGATORIO O CONSIGLIATO O FACOLTATIVO

PRODOTTO	1-2 PC UTENTI	3-5 PC UTENTI	5-10 PC UTENTI	10-20 PC UTENTI	+ 20 PC UTENTI
ANTIVIRUS	O	O	O	O	O
Antivirus centralizzato	O	O	O	O	O
Patch di aggiornamento S.O.	O	O	O	O	O
DLP	O	O	O	O	O
MDM	O	O	O	O	O
Firewall software	O	O	O	O	O
Firewall Hardware	O	O	O	O	O
UTM perimetrale	O	O	O	O	O
Criptazione mobile	O	O	O	O	O
Criptazione Fissa e mobile	O	O	O	O	O
Backup locale	O	O	O	O	O
Backup cloud	O	O	O	O	O
Backup ibrido	O	O	O	O	O
USB con codice o impronta	O	O	O	O	O

In questo corso andremo a conoscere, capire e acquisire le regole e i principi fondamentali del GDPR, attraverso una serie di informazioni specifiche che vi permetteranno di formare la vostra realtà aziendale secondo le disposizioni contenute e richieste dall'art. 29 del regolamento Europeo.

Ti diamo il benvenuto nell'Accademia Virtuale di FastMarketWeb!

Stai partecipando al programma formativo "***I Principi Generali della sicurezza***": questa sessione vi permetterà di capire e conoscere i fondamenti di base del GDPR, che sono diventati obbligatori per tutte le aziende.
In questo modulo di formazione troverete i principi generali del GDPR, i protagonisti, le regole e tutte le funzioni obbligatorie all'interno della gestione organizzativa della vostra azienda che si occupa della raccolta, elaborazione e gestione di tutti i dati personali.

Analizzeremo:

- Chi sono gli interessati;
- Quali diritti hanno;
- Come devono essere gestiti i dati;
- Quali sono le condizioni minime per la protezione ambientale;
- Le specifiche contrattuali;
- Le condizioni di sicurezza e la formazione necessaria all'interno della vostra azienda;
- Quali sono le figure minime da incaricare;
- Le disposizioni di legge, di formazione e d'incarico per ogni figura professionale che lavora con la vostra azienda;
- Le responsabilità e le sanzioni che possiamo affrontare se non siamo ben preparati nel mondo del GDPR.

PRINCIPI GENERALI: le basi delle condizioni minime di attuazione del GDPR.

PREMESSA
GDPR, l'acronimo di General Data Protection Regulation, è il Regolamento Europeo per la protezione e la gestione dei dati personali, entrato in vigore il 25 maggio 2018 e nato ad aprile 2016 come Regolamento Europeo.
Tutte le aziende in Europa devono essersi adeguate alle normative disposte dai 99 articoli del GDPR.

Dal 26 maggio 2018, anche in Italia sono iniziati i controlli da parte dell'organo preposto, la Guardia di Finanza, la quale ha il compito di verificare l'attuazione del Regolamento Europeo. Nel caso in cui ci siano aziende non conformi, gli enti incaricati sono obbligati ad attuare sanzioni in due modi differenti:

- **sanzione amministrativa** per tutti coloro che non trattano dati particolari;
- **sanzione penale** per tutti coloro che trattano dati particolari.

Dal 2016, in ogni Stato membro dell'Unione Europea nasce il GDPR, a esso sono connessi 99 articoli che non hanno delle regole operative generiche, bensì delle disposizioni minime di sicurezza per garantire che tutte le informazioni e i dati aziendali siano accuditi e gestiti secondo il regolamento.

L'osservanza del Regolamento è necessaria affinché durante un controllo i responsabili possano spiegare la modalità di gestione della privacy: se in modo digitale oppure cartaceo. Utile a dimostrare la sicurezza dei dati è il processo di "**privacy by design**", cioè il disegno di tutto il flusso operativo dei dati.
Tale finalità permette poi di comunicare le violazioni qualora siano stati danneggiati oppure rubati i dati gestiti.

GDPR vuol dire sicurezza.
Ogni organizzazione deve aumentare il livello di sicurezza dei PC e della conservazione dei documenti del personale dell'azienda stessa.
La direttiva è stata adottata per salvaguardare il diritto fondamentale della persona, la protezione dei dati e garantirne la libera circolazione all'interno della Comunità Europea.
Negli ultimi 10 anni il nostro modo di comunicare, trasmettere e acquisire i dati è cambiato.
Grazie all'evoluzione delle tecnologie si è discusso il tema della sicurezza, consentendo alle imprese private e alle autorità pubbliche di utilizzare i dati personali in maniera sempre più semplice e definita.

E' necessario installare un quadro giuridico più solido e più coerente in funzione della protezione dei dati all'interno dell'Unione Europea, affinché tutto ciò possa garantire alle persone il controllo dei loro dati personali e rafforzare i principi della loro sicurezza.

Il GDPR è formato da 173 note e 99 articoli. Le note sono importanti perché l'Unione Europea ha voluto creare

delle precisazioni al fine di poter definire e chiarire un determinato articolo, offrendo a tutti gli interessati, una spiegazione sugli aspetti di cui tener conto.

Nella parte finale del corso on-line ci sarà la possibilità di scaricare direttamente la copia personale del Regolamento, messa a disposizione gratuitamente dalla Comunità Europea, al fine di capire come prestare consenso a un trattamento all'interno di una lettera privacy.

Quando si acquisisce un dato, il consenso da parte dell'interessato al trattamento è l'elemento cardine all'interno del GDPR.
Il nuovo regolamento impone il dovere di predisporre delle informative che siano facilmente comprensibili. Ogni singola società deve fornire una serie d'informazioni utili all'interessato, al fine di far comprendere e accettare le condizioni che si pongono per il trattamento del dato stesso.
Un altro elemento fondamentale all'interno del GDPR è il ***Data Breach Notification***, in altre parole, in caso di violazione, furto o perdita dei dati che sono in possesso, bisogna predisporre entro 72 ore dall'accaduto una segnalazione all'organo competente, spiegando e denunciando chi ha fatto cosa.

Il titolare dell'azienda o il responsabile del trattamento deve garantire la sicurezza e la tutela di ogni utente, che sia dipendente, cliente o fornitore.
Se si è proprietari di un Bed and Breakfast e, i clienti con prenotazione, hanno fornito dei dati che comprendono la loro identità, il metodo di pagamento e la loro reperibilità, devono essere tutelati al fine di non incorrere in furti o perdita dei dati, qualsiasi persona con cattive intenzioni potrebbe usarli in modo illecito (esempio: utilizzare i dati della loro carta di credito o usare i loro documenti per furto d'identità).
Dal momento in cui avviene una registrazione, si diventa a tutti gli effetti titolari del trattamento dei dati e l'interessato ha diritto di conoscere in modo chiaro ed esaustivo come sono raccolti e conservati, rendendo chiaro il luogo in cui sono trattati, la banca dati in cui sono custoditi e soprattutto come vengono protetti.
Una nota importante in ogni informativa è il **diritto all'oblio** ovvero la condizione di richiedere al titolare del trattamento di cancellare in tempi utili i dati, ci sono alcuni obblighi ai quali non possiamo adempiere totalmente, ad esempio i dati fiscali, perché per legge devono essere tenuti per almeno 10 anni.

Data Breach Notification, la notifica di una violazione.

Spesso non ci rendiamo conto che i nostri dati aziendali, ogni giorno vivono e si muovono con noi.
Molti professionisti che lavorano da casa, o con il loro smartphone, consultano ed elaborano i dati in mobilità.
La nostra vita frenetica a volte non ci permette di pensare ai rischi che corriamo, basta inviare una mail ad altri utenti per errore, scaricare dei malware da collegamenti ipertestuali non verificati o per assurdo perdere il nostro telefonino o il nostro computer. Quante volte ci è capitato di perdere la nostra agenda? Nel 2020 non possiamo più scherzare, in caso di violazione, perdita o furto dei dati dobbiamo tutelare gli utenti che ci hanno fornito il loro consenso, noi siamo i responsabili e dobbiamo proteggere i nostri database.

I nostri database sono composti d'informazioni riguardanti colleghi, dipendenti, clienti e fornitori.
Il nuovo Regolamento Europeo, obbliga, entro 72 ore, a compiere una comunicazione al Garante per comunicare la violazione subita, specificando la modalità e la tipologia di dati che sono stati violati.

Facciamo un esempio:
La condivisione dei dati con il commercialista, settimanale o mensile, come ad esempio una fattura contenente più informazioni di uno stesso destinatario, può comprometterne la sicurezza se non tutelata correttamente.
Qualsiasi dato può essere utilizzato da un malintenzionato per emettere comunicazioni false, richiedere a terze economie per finte vendite o acquistare prodotti, per questo il GDPR è obbligatorio e va seguito a rispetto degli articoli contenuti nel regolamento.

Qualora non fosse garantito il corretto trattamento dei dati, in caso di controlli o segnalazioni riguardanti violazioni o perdite, s'incorre in sanzioni.
Infatti, ogni qualvolta si debba condividere un dato all'esterno di un'azienda, bisogna far sottoscrivere una lettera d'incarico in cui saranno disciplinate le condizioni, le modalità, le garanzie e le finalità del trattamento che sarà utilizzato.
Le novità introdotte nel GDPR sono molteplici:

- L'art. 32 impone alle aziende la pseudonimizzazione: ovvero una garanzia minima di sicurezza digitale dei dati con conseguente ripristino degli stessi.
- L'art. 4 definisce il dato come un'informazione riguardante la persona fisica, identificata o identificabile: oggi è possibile identificare una persona con un nome, un numero di telefono, un numero d'identificazione o anche un codice particolare che ci permette di acquisire i dati come l'ubicazione, l'indirizzo, un'e-mail o codice fiscale,
- I dati sensibili dell'ex normativa privacy, oggi si chiamano dati particolari e devono essere conservati all'interno di applicativi con molta cura, poiché l'interessato fornisce la sua autorizzazione nel registrare o acquisire

informazioni di origine molto personale,

- L'art. 9 stabilisce quelli che sono i dati particolari (i dati razziali, di etnia, le convinzioni religiose, politiche, filosofiche, lo stato di salute o la vita sessuale di una persona) e quando è vietato trattare dati personali (salvo che l'interessato ci abbia fornito un consenso esplicito totale o parziale per assolvere gli obblighi per cui sono stati autorizzati e nello specifico con ogni singola autorizzazione per la finalità concordata, purché il consenso abbia valenza scritta e non verbale in caso di controllo).
- I dati biometrici e sanitari devono essere trattati con estrema cura, in quanto possono pubblicare informazioni che potrebbero ledere sotto tanti punti di vista coloro che ce li hanno concessi, esempio pratico, immaginiamo che un famoso manager a seguito di un controllo possa ricevere un dato di salute negativo, qualora il dato potesse diventare pubblico senza la sua autorizzazione, potrebbero nascere delle forti ripercussioni sulla sua azienda e sulla sua attendibilità, creando un danno finanziario.

I SOGGETTI DEL GDPR

1) ***Il DPO*** (Data Protection Officer) è la nuova figura competente in relazioni giuridiche e informatiche. Autorizza il trattamento dei suoi dati a un'impresa o a un professionista, ha la responsabilità della gestione dei dati personali, verifica gli strumenti che sono utilizzati per la gestione, ha il compito principale di mettere in atto delle misure tecniche e organizzative che hanno un preciso scopo di garantire e dimostrare la loro sicurezza e soprattutto che il trattamento che è effettuato utilizza una procedura conforme al regolamento secondo i minimi o massimi requisiti di sicurezza necessari. Deve essere nominato obbligatoriamente nel momento in cui in un'azienda i dipendenti siano superiori o pari a 250.

2) ***Il titolare del Trattamento o Data Controller***, è una persona fisica o giuridica cui stata demandata la responsabilità della gestione del dato all'interno dell'azienda, ad esempio può essere colui cui competono le decisioni, le finalità e i modi organizzativi della privacy;

3) Il titolare del trattamento nomina il ***Data Processor*** che ne diventa responsabile: il commercialista, ad esempio, gestisce i nostri dati, bisogna nominarlo come il responsabile al trattamento perché sa del dato integro e lo gestisce al fine di profilare o emettere comunicazioni che contengono di base i dati personali, ma alcune volte possono essere presenti anche condizioni di dati che rientrano come dati particolari. L'art. 83 del GDPR specifica la responsabilità del trattamento da parte del titolare, nel momento in cui quest'ultimo nomina il DPO non risponde per il danno cagionato o per negligenza dal suo lavoro, ma risponde per il danno causato solo se non ha adempiuto gli obblighi presenti nel trattamento.

Il titolare del trattamento dovrà sempre consegnare a tutti gli interessati l'informativa.

4) ***Data Officer***, ovvero il responsabile della protezione dei dati.

GDPR è disciplina, garanzia, metodo e sicurezza.
Ogni azienda deve garantire che i dati degli interessati siano elaborati e gestiti in piena sicurezza sia all'interno dell'azienda sia all'esterno. Oggi è obbligatorio adottare delle misure di prevenzione e cura: i dipendenti devono essere debitamente formati su tutte le procedure di mantenimento e protezione dei dati poiché è importante sapere che il GDPR non essendo un'entità statica, impone che le disposizioni all'interno dell'azienda debbano essere sempre aggiornate secondo le regole che emergono.
Siccome il regolamento è strutturato in maniera molto dinamica, si modifica in funzione delle novità legislative e delle tecnologie che fanno sì che l'interessato possa essere sempre tutelato secondo i minimi standard richiesti.
Per essere totalmente tutelati è necessario far firmare una lettera d'incarico o di nomina (che dovrà essere siglata tra le parti e custodita nella documentazione relazione del Gdpr) a qualsiasi professionista o dipendente che collaborando con la nostra realtà possa raccogliere, elaborare, gestire i dati dei nostri interessati.
Ad esempio: in una realtà aziendale ci s'interfaccia ogni giorno con diverse figure professionali esterne alla vostra azienda, quali il commercialista, il consulente del lavoro, Il medico competente per le visite interne ai dipendenti ecc., queste sono tutte le figure che potrebbero essere coinvolte nella responsabilità dei dati e si richiede stipulare un contratto in maniera molto chiara, rendendo comprensibili i punti che devono essere gestiti, la responsabilità di svolgere determinate azioni, la garanzia e l'impegno alla riservatezza delle informazioni.

Si consiglia che tra la società e l'interessato esista una filiera trasparente: ovvero richiedere a tutti i collaboratori esterni, la loro documentazione relazionale al GDPR, purché si esiga la massima trasparenza e la massima fiducia, poiché il collaboratore cui ci si affida sia totalmente "compliance" al Gdpr, per osservare al meglio i minimi requisiti di sicurezza imposti attraverso la documentazione che è consegnata.
Tutti i dati sono riservati e sono di proprietà aziendale, qualora fossero utilizzati per usi esterni chi di competenza sarà sanzionato in maniera penale o amministrativa.

Trasparenza

Trasparenza è la parola "chiave" del nuovo GDPR.
Se si utilizzano formati elettronici per acquisire consensi per la privacy, bisogna fare attenzione al metodo di raccolta, si richiede:

- Di far leggere all'interessato nella sua totalità le condizioni contenute nella lettera privacy,
- Di tutelarsi sulla tipologia di utente come minorenne o maggiorenne,
- Di far comprendere se i dati che sono raccolti sono dati personali e qualora si acquisisse un dato particolare, per ognuno di questi, vi deve essere la condizione di accettazione e consenso specifica di ognuna.

L'art. 12 determina il principio di trasparenza e impone che le informazioni destinate al pubblico o all'interessato debbano essere facilmente accessibili e di facile comprensione con linguaggio semplice e chiaro.

Esempio:
Il sito internet di un'azienda contiene un formato elettronico di richiesta con nome, cognome, codice fiscale, e-mail, indirizzo e anche dei dati che non servono, per questo nasce il principio di minimizzazione, ovvero si possono raccogliere i dati minimi, esclusivamente utili, mostrando le finalità facendo aderire l'interessato attraverso un "flag" in cui dà il consenso.

Il nuovo GDPR non transige, saranno verificate, con il principio della trasparenza, tutte le condizioni alle quali l'interessato ha dato il suo consenso esplicito con una firma o attraverso il principio di liceità.

Con il GDPR nasce la certificazione: al fine dell'osservanza del regolamento, bisogna avvalersi di meccanismi di certificazione, sigilli e strumenti di protezione dei dati sia digitali sia fisici, che consentono di definire il livello di protezione di dati e di avere più sicurezza da garantire ai clienti o agli interessati.

L'art. 13 chiarisce che nel momento in cui dati personali sono contenuti all'interno di un'azienda, il titolare del trattamento, deve fornire all'interessato le seguenti informazioni:

- Il periodo di conservazione dei dati,
- Sancire i criteri che saranno utilizzati per determinare la condizione finale per la quale sarà definito il termine di utilizzo.

In tutte le informative privacy, il titolare del trattamento, deve garantire l'accesso ai dati all'interessato, nel momento in cui ha bisogno di modificare i dati, comunicando le intenzioni tramite un indirizzo e-mail.
L'esistenza del diritto di revocare il consenso deve essere, per l'interessato, la prima condizione specificata in ogni lettera privacy. Chi gestisce i dati sui minori richiede l'esplicito consenso da parte dei genitori o di chi ne fa le veci.

Qualora la raccolta del dato dovesse essere esclusivamente in modo elettronico, si consiglia di attivare un processo di verifica e autenticazione a due fasi:

1) Un e-mail seguita da un messaggio sms, a questo punto l'utente che riceve due codici distinti può completare il suo consenso disponendo quindi della controprova dei dati che ci ha fornito;
2) Mantenere la prova che abbiamo ricevuto da parte dell'interessato per tutta la durata dell'attività.

.

Sicurezza dei Dati

In questo modulo si prende in considerazione quella che è la sicurezza dei dati.

<u>Che cosa significa per il GDPR un dato sicuro?</u>

Un dato sicuro è tale solo quando si può rispondere in modo certo a ciascuna delle seguenti domande:

1. Dov'è il mio dato? Si trova in Unione Europea o al di fuori dell'Unione Europea?
2. Dov'è custodito? In azienda, in casa, in forma cartacea o all'interno di un database, in un server, in un PC o in un cloud?
3. Per quanto tempo? Un altro punto fondamentale è per quanto tempo è trattenuto questo dato.
4. Chi lo vede questo dato? Chi è incaricato per la sua elaborazione e gestione? A chi può essere ceduto?
5. Quali sono le persone che gestiscono questi dati?
6. Chi sono i soggetti incaricati all'interno del trattamento?
7. Come sono identificati?

La sicurezza del dato e del suo trattamento è disciplinata nell'art. 24 del GDPR e chiarisce che il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate al fine di proteggere il dato e deve essere in grado di dimostrare che il trattamento dei dati personali è effettuato in maniera conforme al Regolamento Europeo.
Nell'art. 32 si parla invece di sicurezza del trattamento, come l'adozione della cifratura dei dati personali, che permette di assicurare la continua riservatezza, l'integrità e disponibilità dei dati personali nei sistemi elettronici adottati nell'azienda.

Un punto importante che, tutte le aziende, che trattano servizi devono garantire, è la capacità di ripristinare in maniera tempestiva e sistematica la disponibilità all'accesso di questi dati, questa modalità è una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure che sono state adottate.

Si ricorda l'importanza del *Data Breach* che, come già discusso, è il sistema di notifica contenuto nell'art. 33, che permette di notificare la violazione dei dati all'autorità di controllo, cioè al garante della privacy, entro 72 ore.
Gli elementi della notifica, cioè che cosa deve contenere l'informazione da inviare al garante, in primis, sono:

- La natura della violazione dei dati personali,
- Quali dati sono stati persi e a chi appartengono,
- Specificare la condizione: ad esempio attraverso un incendio, attraverso un incidente, un furto, un accesso abusivo fisico o digitale da parte di qualche pirata informatico.

L'art. 34, evidenzia chiaramente che si è obbligati a comunicare agli interessati la violazione accaduta, eseguendo una notifica al garante creando un unico documento con la comunicazione specifica dei dati persi, indicando la tipologia e le condizioni. Una volta effettuata la comunicazione alle autorità, bisognerà comunicare a ogni singolo interessato la condizione accaduta.

IL REGISTRO DEI TRATTAMENTI

Il **registro dei trattamenti**, invece, deve essere presente in ogni singola azienda, in questo registro sono presenti tutte le attività che devono essere svolte per il mantenimento della sicurezza dei dati tramite il quale ogni titolare del trattamento deve verificare che le dovute attività siano state redatte con cura ed efficacia.
Per il regolamento europeo, il responsabile è il titolare del trattamento che deve aver prodotto le seguenti attività:

- La valutazione dei rischi
- La definizione delle misure di sicurezza,
- Le condizioni e misure adottate (chi utilizza i PC, come li utilizzano, quale banca dati è nominata, che tipo di dati sono presenti.)
- I sistemi di sicurezza adottati (come antivirus, firewall e condizioni di ripristino documenti e log automation).

Il registro dei Trattamenti è obbligatorio per aziende con personale superiore ai 250 dipendenti, ma è diventato altamente consigliato per tutte le piccole imprese, giacché è un documento molto importante perché permette di definire la valutazione d'impatto dell'azienda e l'analisi dei rischi per ogni singolo trattamento all'interno della vostra attività.

Il registro, in caso di controllo, permette di valutare la metodologia utilizzata all'interno dell'azienda per la sicurezza dei dati, come il DVR nell'ambito della sicurezza, dove una volta evidenziato il risultato in misura bassa, media o alta si determina il grado di compliance dell'impresa.

La Privacy By Design è la condizione che ogni impresa deve prevedere, portando a termine un'analisi completa delle attività a 360°, dalla raccolta, all'elaborazione, al mantenimento, alla gestione, agli incarichi conferiti e alla sicurezza, al flusso operativo e al sistema di gestione della protezione dei dati che è attuato.

Trattamento di Dati in grande scala

Nell'art. 37 del regolamento, si prevede che, quando il trattamento è compiuto da un'autorità pubblica o da un organismo pubblico, fatta eccezione delle autorità giurisdizionali quando esercitano le loro funzioni, bisogna nominare un DPO, perché le attività che sviluppano, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala.
Il DPO deve essere una figura autonoma nelle sue attività, per cui non può essere influenzata dal titolare o da altre persone che sono all'interno dell'azienda stessa, non deve ricevere nessuna istruzione per quanto riguarda l'educazione dei propri compiti, perché deve essere già in grado di realizzarli in maniera autonoma, dimostrando le sue competenze, con certificati in suo possesso. Inoltre deve far rispettare tutti gli aspetti legati al mondo dell'informatica e della gestione del dato sia ambientale sia digitale, deve sorvegliare sull'osservanza del

regolamento e sulle persone verificando che adottino e rispettino le misure impartite.

Cosa s'intende per trattamento su larga scala?
E' il monitoraggio regolare e sistematico di una grande mole di dati:

a) La cura e il funzionamento di una rete di telecomunicazioni: tale attività richiede una gestione, consultazione dei dati su larga scala, il monitoraggio sui clienti in maniera regolare e definisce la natura e il controllo per potergli fruire il servizio.
b) L'uso da parte di società d'indirizzi di posta per inviare messaggi o reindirizzare comunicazioni promozionali o informative,
c) La profilazione per finalità di valutazione del rischio: ad esempio rischio creditizio, premi assicurativi, l'accertamento di alcune forme di riciclaggio e prevenzione frodi,
d) Servizi di geolocalizzazione che permettono a tutti gli utenti di sapere dove sono e cosa stanno facendo.

Responsabilità e Sanzioni

Ogni giorno possiamo essere esposti a questi termini, perché grazie all'art.77, l'interessato può richiedere i danni arrecatogli per una mancata gestione dei suoi dati.
L'art. 77 prevede come principio generale, il diritto dell'interessato a fare ricorso, citando il titolare del trattamento dei dati in tribunale a seguito della violazione e\o infrazione impropria dei dati personali o dati particolari che sono stati forniti. In funzione del dato acquisito si può incombere in una sanzione onerosa.
Il reclamo può essere esercitato da parte dell'interessato direttamente al garante della privacy.
Il ricorso giurisdizionale dettato dall'art. 78 mette in risalto il diritto di proporre un ricorso qualora l'autorità di controllo accerti che la violazione sia avvenuta e soprattutto se la richiesta sia in armonia In base allo Stato membro in cui è stato violato il dato.
Il ricorso può avvenire nello Stato membro in cui si trovano il titolare e l'interessato o in paesi differenti, perché possono trovarsi in Stati diversi: se il titolare si trova in Italia e gestisce dati che provengono dall'Unione Europea, iscrivendo persone attraverso una newsletter in tutta Europa, com'è in possesso del dato dell'interessato italiano, potrebbe acquisire dati d'interessati esteri. Ad esempio:
L'utente olandese iscritto a una newsletter ci ha concesso il dato che è stato rubato e a seguito creato un danno; l'utente può fare reclamo al garante della privacy in Olanda ma lo può fare anche direttamente al garante della privacy in Italia, perché il gestore dei suoi dati possiede la banca di conservazione in Italia.
Verificate poi le responsabilità, vi saranno ovviamente sanzioni amministrative e anche penali per il danno arrecato.

Al fine di tutelare i titolari del trattamento nascono sanzioni massime e minime in base alla tipologia di dato trattato e in base agli articoli 8, 11 e il 25 sono identificate le caratteristiche del dato:

- I dati massimi sono determinati in base al 4% del fatturato totale annuo, con un massimo di 20 milioni di euro,
- I dati minimi sono determinati in base al 2% del fatturato totale annuo con un massimo di 10 milioni di euro.

Se il trattamento del dato riguarderà i dati particolari, il risarcimento sarà molto più alto. Facciamo presente che non esiste una tabella che vale per tutti gli stati membri, ogni Stato dovrà analizzare caso per caso e fornire quella che è la propria valutazione e il valore del risarcimento.

REGOLE - DEFINIZIONI - PRINCIPI DI BASE - SICUREZZA AMBIENTALE

Modalità di conservazione dei documenti cartacei

Innanzitutto, bisogna porre l'attenzione sulla conservazione dei documenti che contengono dati particolari.
Questo riguarda sicuramente tutti i titolari al trattamento che nelle organizzazioni hanno dipendenti e collaboratori:
Tali documenti devono essere tenuti separati dalle altre categorie (fatture, contratti ecc.) e archiviati con chiusure di sicurezza, il cui accesso è riservato solo alle persone responsabili del trattamento di tali dati.
Il rischio della perdita di riservatezza con un impatto elevato nei confronti dell'interessato, è sempre dietro l'angolo se non si adottano le dovute accortezze.
La responsabilità si conferisce anche agli studi professionali come commercialisti e consulenti del lavoro che trattano dati non particolari, la cui divulgazione, alterazione e perdita di disponibilità possono arrecare un danno all'interessato al trattamento, come per esempio le informazioni contenute all'interno delle dichiarazioni dei redditi, alle quali sono allegati giustificativi di spese, scontrini e ricevute in ambito medico sanitario.
È importante che sia adoperata una misura di sicurezza circa l'organizzazione e gestione di tali dati,

prevedendo l’utilizzo di archivi dotati di chiusura e locali con accesso riservato. Comprensibile è trovarsi in una situazione dove, in un primo periodo (anche un paio di anni), tale documentazione non può essere archiviata senza che la gestione del trasferimento incida negativamente e pesantemente nella gestione delle pratiche e dichiarazione da parte dei professionisti e loro collaboratori.

DOCUMENTI A VISTA - DATI PERSONALI

Definizione di qualsiasi oggetto utilizzabile a fini di consultazione, ricerca, informazione, che sia iconografico, fonico, visivo, testimoniante attraverso scrittura specifica di un concetto. Qualora il dato contenuto dovesse ricondurre a una persona, possa fornire un'identificazione, una prova o convalida in ambito burocratico, amministrativo, medico o giuridico, tale dato diviene personale o particolare e quindi diventa un documento da proteggersi secondo le norme contenute nel nuovo GDPR. Tale documento, non può essere a consultazione pubblica verso terzi senza permesso dell'interessato e del titolare del trattamento.

ACCESSO CON REGISTRO O CONTROLLATO

La possibilità o il diritto di accedere a un luogo, qualora ci sia la presenza di dati personali o particolari, il responsabile/titolare del trattamento deve determinare l'accesso attraverso un controllo che possa essere un registro cartaceo, badge, chiave o qualsiasi altra condizione che necessiti di una convalida da persone autorizzate o da sistemi facente la medesima condizione.

ACCESSO VIETATO

L'impossibilità di accedere a un luogo, all'interno di una realtà professionale o di un'azienda, dove al soggetto è comunicata l'interdizione all'accesso di aree nelle quali sono presenti dati personali o particolari, il responsabile/titolare del trattamento, attraverso comunicazioni visive, comunica la condizione di accesso esclusivamente a persone autorizzate.

CARTELLINE PER PSEUDONIMIZZAZIONE

Per la compliance al Regolamento UE GDPR è importante prestare attenzione anche alla conservazione dei documenti cartacei, soprattutto quelli che contengono dati particolari.
È importante, inoltre, adottare misure di pseudonimizzazione come l'utilizzo di numerazioni (che consentono di non vedere il nome del cliente sulle cartelline di archivio) o la dotazione di sistemi di archiviazione a scomparsa. Quest’attenzione va posta sicuramente nelle aree di accesso a persone esterne alle strutture del titolare del trattamento (intese sia come persone interne che+ non hanno l'incarico di trattare determinati dati, sia persone esterne all'organizzazione, come i clienti, addette alle pulizie, consulenti esterni non incaricati).

Protezione Ambientale Armadi, Contenitori Indicazioni

Secondo la nuova normativa europea, la protezione dei dati deve essere anche fisica. Sino a oggi l'attenzione si è concentrata su informative, autorizzazioni, moduli e consensi. La protezione dei dati personali e sensibili va ben oltre le autorizzazioni e coinvolge tutto il processo di trattamento dei dati. La protezione fisica dei dati è uno degli elementi essenziali del GDPR. Per i documenti cartacei è necessario utilizzare armadi con chiave o doppia chiave.
All'interno dell'unità operativa/lavorativa è possibile usufruire di armadi senza chiave denominati “a vista”, tale struttura è definita come elemento di arredo, un mobile costituito essenzialmente di due fiancate verticali a sostegno di scaffali o di liste trasversali per contenere oggetti, tale complemento non può possedere contenitori con dati sia personali sia particolari, qualora se ne dovesse far uso, si richiede la chiusura dello stesso con ante e serratura.
Vi sono anche armadi per archiviazioni di tipo particolare che rispettano normative e certificazioni antincendio: si tratta di armadi blindati di forte spessore che rispecchiano normative in materia di sicurezza, sono armadi che resistono e proteggono il loro contenuto. Ogni armadio antincendio (ignifugo) è dotato di ante a battente e vari metodi di chiusura con serratura e altri sistemi che garantiscono la sicurezza dell'armadio.
Gli armadi ignifughi sono consigliati in alcuni ambiti di lavoro, dove la sicurezza delle documentazioni archiviate è fondamentale.

REGOLE - DEFINIZIONI PRINCIPI DI BASE - SPECIFICHE CONTRATTUALI

CONSEGNA MANSIONARI GDPR

Il titolare deve consegnare ai suoi dipendenti, collaboratori esterni, consulenti e prestatori d'opera il mansionario debitamente siglato.

Il mansionario, deve essere firmato dal responsabile e dall'interessato, contiene le norme specifiche di comportamento che integrano quelle di carattere generale, citate nelle lettere d'incarico.
Ogni Incaricato, in funzione dei compiti che gli sono stati assegnati dal titolare, è tenuto a osservare e fare presente al titolare eventuali errori ed omissioni.

HTTPS SITO WEB

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati tra i computer e i siti. Gli utenti si aspettano che l'utilizzo di un sito web online avvenga in modo sicuro e privato. Invitiamo, pertanto, ad adottare il protocollo HTTPS per proteggere la connessione degli utenti al sito web, indipendentemente dai contenuti. I dati inviati tramite HTTPS sono protetti tramite il protocollo "Transport Layer Security" (TLS), che fornisce tre livelli di protezione fondamentali:

- ***Crittografia***: i dati scambiati sono criptati per proteggerli dalle intercettazioni, nessuno può tenere traccia delle attività svolte in più pagine o carpire le sue informazioni.
- ***Integrità dei dati***: I dati non possono essere modificati o danneggiati durante il trasferimento, intenzionalmente o meno, senza essere rilevati.
- ***Autenticazione***: dimostra che gli utenti comunicano con il sito web previsto. Protegge da attacchi man-in-the-middle e infonde fiducia negli utenti, il che si traduce in altri vantaggi commerciali.

COOKIE SITO WEB

I cookie sono informazioni immesse sul tuo browser quando visiti un sito web o utilizzi un social network con il tuo PC, smartphone o tablet. Ogni cookie contiene diversi dati come, ad esempio, il nome del server da cui proviene, un identificatore numerico, ecc. I cookie possono rimanere nel sistema per la durata di una sessione (cioè fino a che non si chiude il browser utilizzato per la navigazione sul web) o per lunghi periodi e possono contenere un codice identificativo unico. Il responsabile/titolare del trattamento attraverso le specifiche contenute nella lettera privacy evidenzierà la tipologia del trattamento, le finalità e i diritti dell'interessato.

PRIVACY POLICY SITO WEB

La Privacy Policy (o Informativa Privacy) di un sito web o di un'app, è il documento con il quale gli utenti sono informati sulle finalità e modalità di trattamento dei loro dati personali. Il responsabile/titolare del trattamento, attraverso le specifiche contenute nella lettera privacy, evidenzierà la tipologia del trattamento, le finalità e i diritti dell'interessato.

INCARICHI PRIVACY

Informative, incarichi e nomine dei responsabili interni ed esterni.

A tutti i soggetti, deve essere presentata un'informativa che ragguagli l'interessato al trattamento dei dati circa una serie di aspetti, come ad esempio le finalità e le norme del trattamento cui sono destinati i dati, i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati, gli estremi identificativi del titolare del trattamento, ecc.
Le informative da prevedere dovranno quindi essere molteplici, perché ognuna dovrà contemplare le informazioni specifiche per la categoria d'interessati cui si riferisce (ad esempio, saranno normalmente da prevedere informative diverse per Clienti, Fornitori, Dipendenti, Collaboratori/Professionisti, ecc.).

PRIVACY POLICY SICUREZZA AZIENDALE

Si richiede una policy aziendale perché gran parte dei problemi di sicurezza dei dati è, oggi, cagionato da comportamenti errati, soprattutto nelle realtà aziendali dove la parte tecnica è avanzata e la sicurezza informatica è a un buon livello. In tali ambienti, infatti, gli attacchi informatici sono diretti a generare azioni sbagliate che possono aprire falle in sistemi altrimenti inviolabili. Anche con il GDPR, il ricorso a una policy che vieti, ad esempio, di aprire allegati non attesi, di cliccare su collegamenti fraudolenti, di non rispondere a richieste di credenziali o di codici provenienti da (asserite) banche, servizi postali, società emittenti di carte di credito, potrebbe eliminare alla radice ogni rischio. Per mantenere un quadro sicuro con riferimento alla protezione dei dati, di grandissima utilità e suggeriti anche tra le righe del GDPR, sono documenti contenenti istruzioni, regole o indicazioni di comportamento che possano orientare le attività di chi si trova quotidianamente a trattare dati. La presenza, nella realtà produttiva, di soggetti che trattano i dati che siano istruiti dal titolare o dal responsabile comporta, di default, un innalzamento della sicurezza complessiva dell'ambiente, soprattutto

se le regole sono presentate come stringenti e uniformi.

REGOLE - DEFINIZIONI PRINCIPI DI BASE - SPECIFICHE SICUREZZA:

PREMESSA
Il GDPR UE evidenzia la protezione dei dati personali dal momento dell'ideazione (by design and by default). Detto questo, come implementare i metodi di sicurezza e protezione dei dati è a carico di ogni organizzazione. Ci si aspetta che tutte le ditte seguano i più recenti e migliori metodi.

Patch aggiornamento sistemi operativi

Mantiene tutti i sistemi informatici aggiornati installando automaticamente i patch di sicurezza, permettendo di tenere sotto controllo, grazie alla reportistica, lo stato di sicurezza delle macchine.

Password

La password deve rispettare il principio generale dell'art. 32 del GDPR, quindi deve essere adeguata a proposito del sistema che deve proteggere. Una password deve essere composta di almeno 8 caratteri, non deve contenere riferimenti agevolmente riconducibili all'utente, e deve essere cambiata almeno ogni sei mesi. Nel caso di trattamento di dati sensibili o giudiziari la password deve essere cambiata almeno ogni 3 mesi. Non è possibile stabilire a priori una tipologia di password valida sempre e comunque, cioè applicabile indistintamente a tutti i sistemi. Occorre definire più tipologie di password, da utilizzare, al limite, per gruppi omogenei di sistemi. Una password sicura, in ogni caso, non può prescindere dall'essere sufficientemente lunga, con caratteri speciali, senza riferimenti personali dell'utilizzatore e cambiata periodicamente. Definire delle tipologie di password è una pratica fondamentale per essere compliance e conformi al GDPR.

Antivirus come essere Compliance

Per il nuovo regolamento Europeo si richiede di fornire protezione a tutti i computer. Gli antivirus gratuiti possono avere una propria logica in una protezione domestica dei dati ma non danno garanzie a livello professionale poiché le definizioni dei virus si aggiornano mediamente 7-10 volte al giorno in meno degli antivirus commerciali. Da porre l'accento sulla loro mancanza di protezione proattiva perché offrono performance basiche (assenza di anti-rookit, anti-keylogger, ecc.) e perciò il loro utilizzo è molto sconsigliato nelle aziende e studi professionali.
Viviamo nell'epoca dei randomware, delle criptazioni dei dati e dei furti digitali. L'antivirus è il primo obiettivo di sicurezza, è la prima misura indispensabile per garantire un'adeguata protezione dei dati in nostro possesso. Basato su un'architettura client/server, permette la gestione dei client attraverso policy condivise, consentendo di avere reportistiche dettagliate sullo stato delle macchine e avvisi in caso di rilevamento di rischi. In altre parole l'antivirus centralizzato è gestito da una sola macchina mentre su tutti i PC è presente soltanto un agent che risponde ai suoi comandi. È molto più leggero dei normali antivirus e permette di gestire, controllare, impostare policy, autorizzare o impedire azioni, tutto da una sola postazione.

Firewall come essere compliance

La sicurezza digitale, con il nuovo regolamento Europeo, è d'obbligo. Uno degli strumenti più importanti per il dato digitale all'interno di un'azienda è Il Firewall hardware: un'appliance posta all'ingresso della rete aziendale che offre un'ampia gamma di possibilità nella configurazione di regole veramente avanzate per gestire il traffico in ingresso e uscita della propria rete aziendale.
Secondo l'art. 32 GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, della situazione 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 , che comprende:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
Per questo motivo si ha bisogno di un firewall, in altre parole un membro di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più segmenti di rete, fornendo dunque una protezione esterna che possa compromettere la rete tecnologica di un'azienda.
Basato solitamente su un'impostazione di regole automatiche che garantiscono un valido livello di protezione della rete anche a utenti meno esperti, il Firewall software può permettere la creazione di successive regole personalizzate per gestire il traffico in ingresso e uscita della propria rete aziendale.

Il Backup

Il backup dei dati è necessario e obbligatorio, consiste nell'avere sempre una copia di ogni dato prodotto dall'azienda. Il backup è un'azione preventiva che assicura la continuità aziendale, proteggendo i dati da eventi avversi, errori umani e problemi di tensione elettrica. L'obbligatorietà di avere un back up è comprovata, secondo l'art. 32 la sicurezza del trattamento e le misure richieste sono:
1. la cifratura dei dati;
2. La garanzia di riservatezza, integrità, disponibilità e resilienza dei sistemi;
3. il ripristino tempestivo della disponibilità e dell'accesso dei dati in caso d'incidente fisico o tecnico un adeguato livello di sicurezza per evitare la distruzione, la perdita, la modifica, la divulgazione non autorizzata e l'accesso in modo accidentale o illegale dei dati personali trattati.

II back up può essere locale, cloud e ibrido, ognuna di queste condizioni permette di far diventare la vostra azienda compliance per il GDPR. La condizione di recuperare i documenti importanti, contratti, dati statistici e materiali sono indispensabili per ogni azienda. Il backup dei dati aziendali è importante per l'efficienza di studi e aziende.

TOKENIZZAZIONE DEI DATI

Il GDPR UE descrive la protezione dei dati personali. Detto questo, implementare i metodi di sicurezza e protezione dei dati è a discrezione di ogni organizzazione che segua i più recenti e i migliori metodi.
Ad esempio la criptazione e la pseudonimizzazione sono buoni metodi per assicurare un idoneo livello di protezione.
I dati identificativi dovrebbero essere conservati separatamente e l'organizzazione deve assicurarsi che non possa essere fatto il collegamento con una persona fisica. Un noto tipo di pseudonimizzazione è la funzione flash, utilizzata per mappare dati di ogni dimensione verso codici di dimensioni fisse. Un altro metodo sicuro è la tokenizzazione. In tal caso i dati sono sostituiti con token generati casualmente prima di essere processati. I dati originari e i relativi token sono stoccati localmente e sono controllati soltanto dalla compagnia responsabile per i rispettivi dati. La tokenizzazione è a volte ritenuta più efficiente rispetto alla criptazione poiché non ci sono relazioni matematiche che portino indietro i dati originari. Si ritiene che per i file e i dati non strutturati, la criptazione sia preferibile, mentre nel caso dei dati strutturati quali le basi di dati la tokenizzazione sia migliore.

USB Dispositivi mobili

Per possibili perdite o furti di dati si sconsiglia l'uso di USB senza protezioni. Le pen drive USB e più in generale i dischi di memoria esterni con accesso tramite codice o riconoscimento dell'impronta digitale salvaguardano l'accesso ai dati presenti dalle persone che non siano state autorizzate dall'azienda.

UTM (Unified Threat Management)

Per una protezione perimetrale, la soluzione UTM porta numerosi vantaggi sia nelle piccole-medie imprese e nelle grandi aziende con sedi dislocate su più territori e con dipendenti distribuiti in molteplici uffici e gruppi di lavoro. Adottando questa tecnologia gli amministratori di rete sono facilitati a una gestione più efficiente e produttiva rispetto alle svariate necessità dell'azienda. Posto all'origine della rete aziendale (per questo si parla di protezione perimetrale) l'UTM permette di gestire una molteplicità di funzioni rivolte alla sicurezza aziendale tramite un'unica console di gestione e una sola interfaccia GUI. Consente perciò di raccogliere in un'unica appliance le tante soluzioni di protezione diverse fornite da vendor diversi. L'UTM ha in sé tutto il necessario per la sicurezza informatica: firewall, filtraggio antivirus all'inizio della rete prima ancora che le minacce possano raggiungere server e PC dell'azienda, filtraggio dei contenuti del Web e delle e-mail, application control e funzioni di networking come routing e bilanciamento del carico della banda Internet, il tutto racchiuso in un'unica appliance. Garantisce inoltre facilità d'impostazione, troubleshooting potenziato, e una vista unificata dei criteri di sicurezza dell'intera azienda, minimizzando così i costi legati alla gestione e al tempo d'inattività.

Sicurezza Antifurti e Video Sorveglianza

Lo scopo del GDPR è di garantire a ogni individuo la proprietà dei suoi dati personali. Il regolamento impone quindi a tutte le organizzazioni che li detengono, rendere responsabile tutte le fasi del trattamento e della conservazione dei dati. Il dato acquisito può essere gestito sia in modo cartaceo sia elettronico, grazie all'installazione o uso di un sistema di allarme così che il grado di sicurezza ambientale cresca e proporzionalmente incrementi il livello di compliance aziendale. Il Regolamento generale sulla protezione dei dati (GDPR) è un insieme di regole che disciplina tutti i dati personali conservati da un'organizzazione. La videosorveglianza, che sia a uso privato o pubblico, è sottoposta a regole stringenti volte a tutelare la privacy e le libertà fondamentali delle persone. Un servizio di videosorveglianza determina un valore aggiunto al sistema di sicurezza e proporzionalmente allo stato di compliance di un'azienda. L'utilizzo del servizio di videosorveglianza deve essere gestito secondo delle accurate condizioni, che qualora non dovessero essere

osservate possono determinare sanzioni, si necessità di determinare misure di sicurezza a garanzia della riservatezza dei dati per allinearsi ai dettami del GDPR.

REGOLE - DEFINIZIONI PRINCIPI DI BASE - SPECIFICHE INFORMAZIONE E SICUREZZA:

FORMAZIONE AI DIPENDENTI

Il GDPR prescrive all'art. 29 che chiunque tratta dati personali debba essere stato istruito in tal senso dal titolare o dal responsabile del trattamento. Ciò significa che le aziende devono implementare dei processi formativi che rispondano a requisiti delle misure di sicurezza testabili, verificabili e valutabili per chiunque gestisca dati personali. In caso di violazione si rischiano sanzioni fino a 10 milioni di euro o fino al 2% del fatturato annuo. L'intento è di legare l'effettività del Regolamento alle competenze del personale: non è più possibile considerare la privacy e la protezione dei dati come un mero adempimento documentale e burocratico, perché l'efficacia dei processi aziendali passa dal personale interno formato e culturalmente predisposto. In termini di ROI (Return on Investment) significa investire per migliorare i processi organizzativi, proteggere la reputazione aziendale e ridurre i rischi di sanzioni amministrative. Tutto questo presuppone una progettazione degli interventi formativi basata sulla dimensione, la struttura e il business aziendale, individuando specifiche esigenze formative per rendere effettiva la compliance al Regolamento Europeo.

MAIL INFORMATIVA GDPR CLIENTI FORNITORI

L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato, sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento. Essa è condizione di legittimità del consenso, non tanto per rispetto del diritto individuale a essere informato, quanto del dovere del titolare del trattamento di assicurare la trasparenza e correttezza dei trattamenti fin dalla fase di progettazione, e di essere in grado di comprovarlo in qualunque momento (principio di accountability). L'informativa ha anche lo scopo di permettere che l'interessato possa rendere un valido consenso, se richiesto come base giuridica del trattamento. In questo caso l'informativa non è solo dovuta in base al principio di trasparenza e correttezza.

COOKIE POLICY WEB GDPR

Considerata la particolare invasività che i cookie di profilazione (soprattutto quelli terze parti) possono avere nell´ambito della sfera privata degli utenti, la normativa europea e italiana prevede che l´utente debba essere adeguatamente informato sull´uso degli stessi ed esprimere il proprio valido consenso all´inserimento dei cookie sul suo terminale. In particolare, con il provvedimento "*Individuazione delle modalità semplificate per l´informativa e l´acquisizione del consenso per l´uso dei cookie*" dell´8 maggio 2014, il garante, per la protezione dei dati personali ha stabilito che quando si accede all'home page o a un´altra pagina di un sito web che utilizza cookie per finalità di profilazione e marketing, deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente:

1) che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
2) che il sito consente anche l´invio di cookie di "terze parti", in caso di utilizzo di questo tipo di cookie, ossia di cookie installati da un sito diverso tramite il sito che si sta visitando;
3) un collegamento ipertestuale a un'informativa più ampia, con le indicazioni sull´uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti";
4) l´indicazione che proseguendo nella navigazione (ad es., accedendo a un´altra area del sito o selezionando un´immagine o un collegamento) si presta il consenso all´uso dei cookie.