MZ S.r.l.s. Services

DISPENSE FORMAZIONE GDPR

IL REGOLAMENTO IN BREVE

Il vecchio D.lgs n°196 del 2003 in materia di protezione dati viene sostituito dal GDPR - General Data Protection Regulation, il nuovo regolamento europeo n°679 del 2016 riguardo la privacy con efficacia a partire dal 25 Maggio 2018, che va ad ampliare il campo applicativo introducendo nuovi concetti.
Il GDPR si rivolge ad aziende, associazioni, liberi professionisti, cooperative tutti coloro che trattano dati personali.

Ma vediamo nel dettaglio la differenza maggiore con il vecchio codice di protezione dei dati e l'approccio all'argomento. Mentre il decreto legislativo imponeva una serie di norme dettate dal legislatore, il GDPR ci guida verso un metodo di lavoro preventivo e fornisce l'obbiettivo ultimo della protezione dei dati lasciando al Titolare la responsabilità di trovare la strada più adatta alla propria realtà, definendo delle linee guida, per raggiungere l'obbiettivo posto.

È quindi un regolamento del flusso dei dati sia per salvaguardare il proprietario di essi, sia come catalogazione per un possibile utilizzo interno aziendale. Questo facilita la raccolta e l'utilizzo diminuendo sprechi di tempo e raccolta di dati superflui, facilitandone il ritrovamento.

LE PARTI COINVOLTE

L' AUTORITÀ DI CONTROLLO

È l'autorità Pubblica indipendente istituita dallo stato membro, ai sensi dell'articolo 51. In Italia questa figura è rappresentata dal Garante della privacy. Il suo compito è la verifica che sia stata applicata la norma ed i metodi usati. Si occupa inoltre di sanzionare i trasgressori. È l'autorità alla quale ci si deve rivolgere in caso di fuoriuscita di dati e che riceve ed esamina reclami e segnalazioni.

IL PROPRIETARIO DEI DATI

Il proprietario dei dati è il reale proprietario, la persona fisica, al quale appartengono i dati personali raccolti. I dati raccolti possono quindi riferirsi a clienti, dipendenti, collaboratori, fornitori, chiunque sia a contatto con l'azienda o che fornisca spontaneamente i propri dati.

IL TITOLARE DEL TRATTAMENTO DEI DATI - ART. 24

Si intende per Titolare del trattamento dei dati colui che che definisce le modalità del trattamento, può essere la società o la persona interna ad essa. Può essere una persona fisica, giuridica, autorità pubblica o altro organismo. Colui che determina la procedura, le finalità ed i metodi di raccolta dati seguendo le procedure conformi al regolamento, determina inoltre chi saranno i soggetti autorizzati al trattamento.

IL CONTITOLARE DEL TRATTAMENTO DEI DATI - ART. 26

Questa figura viene nominata nel momento in cui due o più titolari del trattamento sono interessati allo stesso trattamento di dati, essi diventano contitolari del trattamento e determinano tramite accordo interno le rispettive responsabilità.

IL DPO O DATA PROTECTION OFFICER - RESPONSABILE DELLA PROTEZIONE DEI DATI - ART 37-39

Il DPO Data Protection Officer è una figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi che viene designato dal titolare del trattamento come responsabile della protezione dei dati, per occuparsi del trattamento

dei dati. Egli dovrà informare e fornire consulenza a coloro che trattano i dati nell'azienda seguendo il regolamento.

Il ruolo di DPO può essere affidato ad una persona interna all'azienda come uno dei dipendenti ma può anche essere esternalizzato ad un consulente.

Un gruppo imprenditoriale, come anche più autorità o organismi pubblici possono designare un solo DPO, tenendo conto della loro struttura per organizzazione e dimensione.

Tale designazione è obbligatoria solo in tre casi:

- Per le amministrazioni e gli enti pubblici
- Se l'attività principale svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala.
- Se l'attività principale svolta dal titolare o dal responsabile del trattamento consiste nel trattamento su larga scala di categorie particolari di dati personali o dati relativi a condanne penali e a reati.
- Se la società ha un più di 250 dipendenti.

IL RESPONSABILE DEL TRATTAMENTO DEI DATI - ART 28

È la persona o l'organizzazione che si occupa del trattamento dei dati all'esterno dell'azienda. Questa figura deve determinare, soddisfando i requisiti del regolamento, le finalità ed i mezzi del trattamento dei dati ricevuti. I trattamenti da parte di un responsabile sono designati tramite contratto o altro atto giuridico. Può trattarsi del consulente del lavoro, del medico competente, dei sistemisti, nella fattispecie coloro i quali trattano, per adempire ad obblighi o per altri scopi, dei dati personali per conto del titolare del trattamento.
Questa persona viene nominata dal titolare del trattamento, tramite apposito documento di nomina.

IL RAPPRESENTANTE DEL TRATTAMENTO DEI DATI - ART. 27

La figura del rappresentante del trattamento è necessaria nel caso in cui un'azienda con sede fuori dall'Unione Europea decida di trattare dei dati interni all'Unione Europea. In questo caso è necessario che il titolare de trattamento designi un rappresentante. Egli si occuperà di informare l'azienda extra UE degli obblighi relativi al GDPR, questa persona è stabilità in uno degli stati membri in cui si trovano gli interessati.

I DATI

RACCOLTA DATI

Ogni titolare del trattamento raccoglie dati necessari all'attività produttiva, i dati interessati del GDPR sono i dati personali. Per i quali intendiamo qualsiasi dato che possa ricongiungere all'entità della persona fisica. Con questo regolamento per esempio i dati delle società vengono quindi esclusi mentre i dati dei loro dipendenti vengono inclusi.

Questi dati possono essere in formato cartaceo o in formato digitale e dovranno essere trattati esclusivamente dalle persone autorizzate.

LE TIPOLOGIE DI DATI

I dati a cui si riferisce il regolamento sono nella fattispecie i **dati personali** e i **dati particolari**.

DATO PERSONALE

Per **dato personale** si intende qualsiasi dato che possa ricongiungere, da solo o con altri dati, all'entità di una persona fisica identificata o identificabile. Per esempio, Nome, Cognome, Codice Fiscale, indirizzo, data di nascita.

DATO PARTICOLARE

Il **dato particolare** invece è qualsiasi dato che si riferisca a opinioni politiche, stato di salute, opinione religiosa, appartenenza sindacale, origine razziale. Appartengono a questa categoria, inoltre: i dati giuridici, genetici e biometrici.

TRATTAMENTO DEI DATI

Il trattamento del dato personale è qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata ai dati personali, come la raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, consultazione, diffusione o cancellazione.

Il GDPR dice che il trattamento del dato deve:
. essere corretto, lecito e trasparente
. serve una base giuridica per trattare i dati di una persona per esempio la prestazione di un consenso
. avere una finalità determinata, esplicita e legittima
. deve essere pertinente, limitato e adeguato
. aggiornato e esatto
. conservare il dato

FREQUENZA DI TRATTAMENTO

OCCASIONALE

Il trattamento può avvenire in modo occasionale se il dato viene trattato una tantum presso uno o più individui, come ad esempio la ricezione di un ordine da un nuovo cliente.

SISTEMATICO

Oppure in modo sistematico se è trattato periodicamente o con scadenze, ad esempio un servizio di mailing list automatizzato e periodico.

PROFILAZIONE

Un altro metodo di trattamento dei dati è la profilazione, ovvero il trattamento automatizzato di dati personali atto all'analisi delle preferenze personali, degli interessi o dell'ubicazione di eventuali clienti.

LUOGO DI UTILIZZO DEI DATI

Alcuni dati vengono raccolti e trattati all'interno dell'azienda. Mentre per altri vi può essere la necessità o volontà di inviarli a terzi.
L'invio di dati personali a terzi è un trattamento contemplato, basta che il proprietario dei dati sia informato e abbia dato il proprio consenso in maniera inequivocabile. Al contrario di quanto si pensi l'obbiettivo del GDPR è quello di favorire la circolazione dei dati ed è grazie alla regolamentazione dei trattamenti che questa cosa è possibile.

IL METODO DI TRATTAMENTO

I dati raccolti dalle aziende, per essere in regola con il GDPR, dovranno essere trattati con diverse modalità a seconda della categoria a cui appartengono. Il titolare del trattamento o il DPO potranno gestire il trattamento dei dati in modo più consono alle necessità dei Titolari del trattamento e le realtà in cui operano.
Ecco alcuni punti da seguire a seguito della raccolta dei dati da parte del titolare del trattamento:

- DESCRIZIONE DATI TRATTATI

Descrizione di che tipo di dati sto trattando e quali (es. nome, cognome, indirizzo bancario, ecc.)
Dovrà quindi descrivere il tipo di dato trattato (personale e/o particolare, la modalità del trattamento e se sono presenti dei contitolari o responsabili del trattamento.

- ASSETS

Salvataggio e catalogazione dei dati in un luogo prestabilito.
Verrà quindi definito dove i dati verranno raccolti e mantenuti.

- FINALITÀ

Per cosa vengono utilizzati questi dati?
Saranno indicate le finalità per le quali i dati sono stati raccolti e trattati, per esempio statistiche aziendali, campagne pubblicitarie o profilazione.

- PROPRIETARI DEI DATI

Di chi sono i dati trattati?
Saranno indicate le categorie degli interessati, coloro che sono i proprietari dei dati.

- DURATA

Per quanto tempo verranno mantenuti i dati?
Dovrà essere indicato per quanto tempo verranno mantenuti i dati

- DESTINATARI

A chi vengono comunicati i dati?
Sarà indicato a chi saranno trasmessi i dati e se sono presenti Contitolari e Responsabili dei dati.

- MISURE DI SICUREZZA

Come vengono protetti i dati?
É obbligatorio indicare come verranno protetti i dati e le modalità di backup. Per questo consigliamo di far predisporre un elenco dei sistemi di sicurezza da chi vi segue la parte informatica, ad esempio backup, antivirus e la gestione di eventuali credenziali di accesso ai PC.

REGISTRO DEI TRATTAMENTI - ART.30

Dovrà quindi essere fornito un documento esplicativo chiamato registro dei trattamenti contenente le informazioni dettagliate del metodo di trattamento e catalogazione dati utilizzati, riassumendo tutti i trattamenti in un unico documento.

LE POSSIBILI SANZIONI

Con il GDPR le sanzioni Penali previste dal vecchio Decreto vengono eliminate, ma le sanzioni amministrative vengono inasprite, queste possono variare da richiami a vere e proprie multe da parte dell'organo che si occupa di sanzionare, ovvero come abbiamo visto, il Garante della Privacy.

Le sanzioni possono essere fino a:

- 10 milioni di € o 2% del fatturato annuo per: mancata applicazione di misure di sicurezza, trattamento illecito di dati personali, mancata o errata comunicazione di un data breach all'Autorità nazionale competente.

-20 milioni di € o 4% del fatturato per: trasferimento illecito di dati personali ad un destinatario in un Paese terzo oppure inosservanza di un ordine di limitazione imposto DA un'Autorità nazionale competente.

I DIRITTI DEGLI INTERESSATI

Il GDPR presenta nuovi diritti per i proprietari dei dati personali.

DIRITTO DI ACCESSO - ART 15

L'interessato ha il diritto di essere a conoscenza di un eventuale trattamento dei dati in corso e può avere accesso alle seguenti informazioni: finalità del trattamento, categorie di dati personali in questione, destinatari dei dati, durata di conservazione, origine dei dati e deve essere messo a conoscenza del diritto di rettifica, cancellazione o possibile reclamo alle autorità. Se i dati vengono trattati in paesi terzi ha il diritto di avere informazioni e garanzia sulle modalità di trattamento.

DIRITTO DI REVISIONE E CORRETTEZZA

L'interessato ha il diritto di poter revisionare in qualsiasi momento i propri dati e che questi dovranno essere corretti e forniti il prima possibile, cosicché eventuali terzi abbiano i dati sempre aggiornati.

DIRITTO DI RETTIFICA - ART. 16

L'interessato deve poter far sostituire o ottenere un'eventuale integrazione dei dati forniti, quando viene fatta richiesta.

DIRITTO DI CANCELLAZIONE/DIRITTO ALL'OBLIO - ART 17

È la facoltà dell'interessato di fare cancellare, o far si che i dati riguardanti la sua identità non siano più utilizzati dal titolare del trattamento, nel caso in cui i dati siano stati divulgati a terzi è necessario che il titolare faccia richiesta di cancellazione di tali dati ad altri titolari del trattamento che se ne sono occupati, in caso che questa azione non comporti un dispendio eccessivo di tempo e denaro.

DIRITTO DI LIMITAZIONE DEL TRATTAMENTO - ART 18

Il proprietario è libero di decidere in che misura far trattare i propri dati.

per esempio, se vi sono più scopi, il titolare dovrà informare e far decidere liberamente al proprietario le finalità del trattamento.

Facendo attenzione che una mancata risposta non è da considerarsi come silenzio assenso, quindi dovremo avere una risposta verbale o scritta.

DIRITTO DI OPPOSIZIONE - ART. 21

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati, compresa la profilazione. Ha inoltre il diritto di opporsi ad un trattamento con finalità di marketing, a fini di ricerca scientifica, storica o di dati statistici salvo il caso i cui i dati vengano raccolti per l'esecuzione di un compito di interesse pubblico.

DIRITTO DI PORTABILITÀ - ART 20

L'interessato ha il diritto di ricevere, da un titolare del trattamento, i dati personali forniti (in un formato leggibile) per trasmetterli a un altro titolare del trattamento. L'interessato ha inoltre il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro se tecnicamente possibile. Sono portabili solo i dati trattati con il consenso dell'interessato o che siano stati forniti dall'interessato.

VALUTAZIONE DEI RISCHI

I rischi riguardanti la violazione della privacy possono variare in base alle tipologie di dati trattati, poiché se verranno sottratti dei dati particolari sarà più grave rispetto ad una violazione dei dati personali, cosi come una violazione dei dati giuridici potrà essere considerata molto grave.

Tra i maggiori rischi possiamo evidenziare

VIOLAZIONE

In caso vengano bypassati i sistemi di sicurezza e vengano trafugati i dati trattati all'interno dell'azienda.

PERDITA DI INTEGRITÀ

In caso vengano danneggiati, sia per attacco hacker o per qualche danneggiamento durante l'utilizzo aziendale.

PERDITA DI DISPONIBILITÀ

In caso vengano persi o bloccati in modo definitivo, una soluzione potrebbe essere ad esempio avere dei backup periodici dai quali ripristinare i dati

Va tutto valutato a seconda della tipologia e di come vengono trattati i dati, poiché in alcune realtà i rischi potranno essere maggiori e quindi la protezione dei dati andrà approfondita e gestita in modo più efficace.

MISURE PREVENTIVE

Cercare di agire in prevenzione è il concetto essenziale di questo regolamento, è stato definito "Privacy by Design" ovvero i problemi vanno valutati nella fase di progettazione poiché si evitino perdite di dati inutili e non vi siano rischi o sanzioni. **ART 23-25**

ACCOUNTABILITY

L'accountability è il concetto chiave di questo regolamento, ovvero la responsabilizzazione nell'adottare le misure preventive necessarie alla protezione dei dati, nei progetti e nei piani futuri implementando quelli esistenti. Viene quindi affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative.

PRIVACY BY DESIGN

È la necessità di configurare il trattamento in anticipo, prima che avvenga la raccolta dei dati. Così facendo verranno adottate misure tecniche e ci si sarà organizzati adeguatamente prevenendo eventuali rischi per i dati.

PRIVACY BY DEFAULT

Poiché si cercherà di raccogliere i dati strettamente necessari alle finalità del trattamento, cercando di evitare dati superflui.

diminuendo i dati posseduti si diminuiscono quindi i rischi.

MISURE PREVENTIVE ADOTTATE DAL TITOLARE DEL TRATTAMENTO

Possono essere:

PSEUDONIMIZZAZIONE E CIFRATURA

Si utilizza per la protezione dei dati personali facendo in modo che gli stessi non siano attribuibili ad una persona fisica identificata o identificabile, andando quindi, per esempio, a sostituire un nome con un numero.

CRITTOGRAFIA

Si utilizza per rendere i dati illeggibili a persone non autorizzate, tramite programmi appositi che si basano su un algoritmo di cifratura o in modo più semplice con una password.

PROTEZIONE BACKUP

È possibile proteggere un backup o salvataggio di dati rendendolo sicuro tramite password e protezioni di rete prevedendo l'eventuale chiusura sotto chiave degli stessi.

PROTEZIONE DATI CARTACEI

Se in possesso di dati particolari cartacei questi dovranno essere riposti in archivi sotto chiave.
In molte aziende gli unici dati sensibili da proteggere saranno quelli dei dipendenti, in questo caso saranno da proteggere inserendoli in un archivio protetto da chiave, segnalando chi è in posso della stessa o chi è autorizzato ad accedervi

PROCEDURE IN CASO DI FUORIUSCITA DATI

ART 33

IL DATA BREACH

Data Breach significa violazione dei dati. É obbligatorio comunicare entro 72 ore un'eventuale perdita o fuoriuscita di dati all'autorità competente, il Garante della Privacy, che provvederà ad esaminare il caso ed eventualmente indicare un'eventuale procedura da seguire.

Nel caso in cui la violazione dei dati possa essere un rischio per la libertà o i diritti dell'individuo, il titolare del trattamento dovrà comunicare la fuoriuscita del dato anche all'interessato spiegando l'accaduto in modo chiaro e enunciando la natura della violazione.

Dobbiamo analizzare quindi la natura ed il tipo di dati coinvolti nella violazione, Per esempio la fuoriuscita di dati di un ospedale può essere un grave pericolo per la privacy del paziente perché coinvolgono i dati riguardanti la sua situazione sanitaria è quindi necessario che il titolare del trattamento comunichi questa perdita all'interessato.

È necessario tener traccia dei casi di violazione allo scolpo di individuare i fattori di rischio e poter migliorare la sicurezza dei dati.

CRYPTOLOCKER E RISCATTI

Il cryptolocker è un altro esempio di violazione ma avviene tramite una perdita di disponibilità dei dati mediante crittografia da parte di terzi (hacker), gli stessi richiedono, nella maggior parte dei casi, un riscatto per rendere nuovamente leggibili i file, tale riscatto potrà avvenire normalmente tramite pagamento oppure in bitcoin.

Sovente questi cryptolocker si insidiano in allegati formato zip. di e-mail, il consiglio è porre particolare attenzione ai domini degli indirizzi da cui arrivano queste mail.

CONSENSI E INFORMATIVE

IL CONSENSO - CONDIZIONI DI LICEITÀ - ART. 6

Ogni trattamento deve trovare una base giuridica come ad esempio l'espresso consenso da parte dell'interessato.

Il consenso del trattamento dei dati, non è necessario nel caso in cui il trattamento avvenga per l'esecuzione di un contratto, così come per l'adempimento di un obbligo legale, poiché rispetta la condizione di liceità.

É necessario il consenso esplicito al trattamento dei dati da parte dell'interessato nel caso in cui si trattino dati particolari, per interessi diversi a scopi legali o contrattuali, o dati con trattamento automatizzato inclusa la profilazione.
Il consenso deve essere libero, specifico, informato che sia sufficientemente chiaro lo scopo e le finalità. Ed inequivocabile Non è ammesso il consenso tacito o presunto, necessiteremo per forza di una risposta, in caso contrario è da considerare come un no alla richiesta

Non deve per forza essere documentato per iscritto anche se con un documento cartaceo è più facile dimostrarne il consenso, in quanto il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il consenso.

Qualsiasi consenso percepito prima dell'entrata in vigore del GDPR può essere ritenuto valido se ha le caratteristiche sopra elencate e non è stato modificato.

CONSENSI DAI MINORI

Parlando di minori occorre fare due distinzioni, il consenso di minori dai 16 anni di età è da considerarsi valido, al di sotto invece dei 16 anni è necessario avere il consenso dei genitori o di chi ne fa le veci.

L' INFORMATIVA

CONTENUTI INFORMATIVA - ART. 13-14

L'informativa da fornire all'interessato di cui sono stati raccolti i dati deve contenere:

- l'identità e i dati di contatto del titolare del trattamento
- eventualmente del suo rappresentante e del responsabile della protezione dei dati
- i motivi e le finalità del trattamento
- eventuali destinatari
- le categorie a cui appartengono
- specificare se i dati possono essere trasferiti a un paese terzo e attraverso quali strumenti

Inoltre va specificato:

- il periodo di conservazione
- i diritti dell'interessato di accesso, cancellazione, limitazione, revoca di consenso e possibilità di reclamo
- se la comunicazione dei dati è obbligatoria per la chiusura di un contratto è obbligatorio specificare le conseguenze di una mancata comunicazione
- specificare se i dati verranno sottoposti a profilazione specificando anche la logica di tali processi decisionali e le conseguenze per l'interessato

TEMPISTICHE PER FORNIRE L'INFORMATIVA

Nel caso in cui i dati sia raccolti presso l'interessato l'informativa va fornita prima della raccolta di questi e deve comprendere anche le categorie dei dati personali oggettO di trattamento; invece nel

caso in cui i dati non vengano raccolti presso l'interessato l'informativa deve essere inviata entro 1 mese della raccolta.

SITI WEB & SOCIAL NETWORK

SITI WEB

Per i siti web dovremo andare a modificare la privacy policy presente obbligatoriamente sul sito, con le diciture del nuovo regolamento, informando i navigatori di tutti i cookies ed altri processi che raccolgono dati durante la navigazione ed il loro eventuale utilizzo.

Inserendo una sezione, se necessario, per i consensi per tutti gli eventuali utilizzi dei dati.

Per esempio se richiediamo un'iscrizione, e i dati di chi si iscrive saranno utilizzati per mandare informazioni e marketing, dovremo chiedere il consenso per tutte e due le finalità, indicando cosa possa comportare il mancato consenso.

SOCIAL NETWORK

Il GDPR non fornisce indicazioni specifiche all'utilizzo dei social network. Ogni social provvede a trattare i dati che raccoglie al suo interno secondo il GDPR. il prelevamento di dati dai social network può essere riconducibile all'art.14 di detto regolamento dove vengono descritte le informazioni da fornire in caso i dati non siano raccolti direttamente dall'interessato. Nel caso in cui una società raccolga dei dati per utilizzarli all'esterno dei social network come per esempio raccogliere contatti per vario utilizzo.

In questo caso si dovrà fornire all'interessato, entro un mese dalla raccolta dei dati, le seguenti informazioni:

Dove sono stati raccolti, finalità, categorie di dati ed eventuali destinatari

Per garantire un trattamento corretto il titolare dovrà andare a fornire anche le seguenti informazioni:

Diritti dell'interessato, periodo di conservazione e se presente un processo di profilazione.