Ordine degli Ingegneri della Provincia di Isernia

SEMINARIO DI FORMAZIONE

La privacy: le novità introdotte dal Regolamento Europeo 679/2016 e gli obblighi per l'ingegnere

Isernia – 30 novembre - 1 dicembre 2018

FEDERPRIVACY FEDERAZIONE ITALIANA PRIVACY

Dott. Guido Savelli - Consulenze Privacy

Privacyitalia

Cos'è la privacy?

Nell'opinione comune il concetto di privacy è considerato come il **diritto alla riservatezza di un individuo, che deve essere rispettato da tutte le persone che hanno a che fare con quest'ultimo.**

Se guardiamo all'interpretazione della norma secondo il diritto anglosassone, il concetto di privacy viene inteso come il ***diritto alla data protection,*** cioè quel **complesso di norme che regolamentano il trattamento dei dati personali di un soggetto (interessato).**

Ciò che viene tutelato dalla legge è il trattamento di qualsiasi informazione riferibile ad un individuo.

INFORMAZIONE = DATO

Che cos'è il DATO PERSONALE

È qualsiasi informazione riguardante una persona fisica, identificata o identificabile (**interessato**); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento ad un identificativo come **il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale**.

Il nuovo regolamento si arricchisce della definizione di dato genetico, dato biometrico, dato relativo alle condizioni di salute.

I dati personali costituiscono la base per le operazioni ad essi connesse. Tali operazioni prendono il nome di

TRATTAMENTO

…qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come **la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione** mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Esistono dei presidi che sovrintendono al trattamento dei dati personali, che noi possiamo denominare principi.

PRINCIPI GENERALI da osservare

- **LICEITA'** ……(rispetto delle norme);
- **CORRETTEZZA**……. (rispetto delle esigenze reciproche, oltre lo stretto dato normativo);
- **TRASPARENZA**…..(assicurare la consapevolezza dell'interessato)
- **LIMITAZIONE DELLE FINALITA' ….** (gli scopi del trattamento devono essere determinati, espliciti e legittimi, trattamenti successivi a quelli iniziali non devono avere finalità incompatibile con quella originaria (salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche)

- **MINIMIZZAZIONE DEI DATI** (i dati devono essere adeguati, pertinenti, e limitati a quanto necessario nel rispetto delle finalità);
- **ESATTEZZA**….. (i dati devono essere esatti e. se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti);
- **LIMITAZIONE DELLA CONSERVAZIONE** ….(i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (salvo trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche);
- **INTEGRITA' E RISERVATEZZA**…. (i dati devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

INFORMATIVA all'interessato (ex art. 13 GDPR)

Elementi da fornire all'interessato:

- Dati del Titolare del trattamento;
- Dati del DPO;
- Finalità del trattamento;
- Destinatari dei dati trattati;
- Periodo di conservazione dei dati e/o durata del trattamento;
- Se vi è una finalità ulteriore rispetto a quella originaria, ne deve essere data informazione all'interessato.

CONSENSO dell'interessato

Alla base del trattamento dei dati personali che investe qualsiasi interessato è INDISPENSABILE che egli manifesti il proprio benestare al trattamento dei dati che lo riguardano = **(CONSENSO).**

Si può definire il consenso come qualsiasi manifestazione di volontà da parte dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva al trattamento dei dati personali che lo riguardano che sia:

Libera, (senza condizionamenti)
Specifica, (relativa esclusivamente al trattamento che si deve mettere in atto)
Informata (che evidenzia conoscenza diretta del trattamento)
Inequivocabile (che esclude qualsiasi riserva o incertezza),

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

Dagli articoli 12 a 23 del regolamento vengono disciplinati i diritti assegnati all'interessato

Il titolare del trattamento fornisce (ex art. 12 GDPR) TUTTE le informazioni relative al trattamento in forma

CONCISA

TRASPARENTE

INTELLEGIBILE

FACILMENTE ACCESSIBILE

Con un linguaggio semplice e chiaro, in particolare nel caso in cui le informazioni siano destinate a minori.

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

1. DIRITTO DI ACCESSO (ex art. 15 GDPR)

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) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

d) quando possibile, **il periodo di conservazione dei dati** personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

1. DIRITTO DI ACCESSO (ex art. 15 GDPR)

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento **la rettifica o la cancellazione dei dati** personali o **la limitazione del trattamento** dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre **reclamo a un'autorità di controllo**;

h) **l'esistenza di un processo decisionale automatizzato**, di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, **informazioni significative sulla logica utilizzata**, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

2. **DIRITTO DI RETTIFICA (EX ART. 16 GDPR)**

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

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

3. **DIRITTO ALLA CANCELLAZIONE (C.D. DIRITTO ALL'OBLIO)** (EX ART. 17 GDPR)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste PRINCIPALMENTE uno dei motivi seguenti:

- DATI NON PIU' NECESSARI
- REVOCA DEL CONSENSO
- OPPOSIZIONE AL TRATTAMENTO senza la sussistenza di alcun motivo legittimo prevalente per procedere al trattamento
- TRATTAMENTO ILLECITO
- CANCELLAZIONE PER ADEMPIMENTO DI UN OBBLIGO LEGALE

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

4. DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO (EX ART. 18 GDPR)

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- l'interessato **contesta l'esattezza dei dati personali**, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- il **trattamento è illecito** e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono **necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria**;
- **l'interessato si è opposto al trattamento** ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

5. DIRITTO ALLA PORTABILITA' DEI DATI (EX ART. 20 GDPR)

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 a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso;

b) il trattamento sia effettuato con mezzi automatizzati.

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

I DIRITTI DEGLI INTERESSATI AL TRATTAMENTO

6. DIRITTO DI OPPOSIZIONE (EX ART. 21 GDPR)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi, compresa la profilazione.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che **prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato** oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali 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 effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

I SOGGETTI NEL PANORAMA DELLA DATA PROTECTION

- **TITOLARE DEL TRATTAMENTO** - l'autorità privata o pubblica che determina le finalità e i mezzi del trattamento
- **RESPONSABILE DEL TRATTAMENTO** – la persona fisica o giuridica che tratta i dati per conto del titolare
- **AUTORIZZATO AL TRATTAMENTO** la persona che tratta i dati sotto l'autorità diretta del titolare o del responsabile

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

1. Principio della **RESPONSABILIZZAZIONE DIRETTA DEI TITOLARI DEL TRATTAMENTO** (accountability e principi della privacy by design e by default)

2. Adozione dei **REGISTRI DEI TRATTAMENTI (e delle attività di tratt.)**

3. Valutazione d'Impatto **(DATA PROTECTION IMPACT ASSESSMENT)**

4. Violazione dei dati personali **(DATA BREACH)**

5. Nomina del **RESPONSABILE PROTEZIONE DATI (DPO)**

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

1. PRINCIPIO DELLA RESPONSABILIZZAZIONE DIRETTA DEI TITOLARI DEL TRATTAMENTO

Il principio appena menzionato comporta la richiesta al titolare del trattamento di **METTERE IN ATTO MISURE TECNICHE ED ORGANIZZATIVE ADEGUATE PER GARANTIRE, ED ESSERE IN GRADO DI DIMOSTRARE, CHE IL TRATTAMENTO VIENE EFFETTUATO CONFORMEMENTE AL REGOLAMENTO**

(è questo il cosiddetto principio dell'**accountability** di cui all'art. 24 del Regolamento).

A questo principio vanno associati altri due principi che l'ente deve necessariamente osservare:

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

PRIVACY BY DESIGN:
cioè **riduzione al minimo del trattamento dei dati** mediante misure tecnico organizzative (es. pseudonimizzazione) con **protezione dei dati fin dalla progettazione**

PRIVACY BY DEFAULT:
cioè che la tutela della protezione del dato deve diventare l'impostazione predefinita. Devono essere trattati, in sostanza, **solo i dati necessari per ogni specifica finalità di trattamento**

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

2. Adozione del REGISTRO DEI TRATTAMENTI (di quello delle attività di trattamento oppure, in sostituzione di entrambi, il Registro Unico dei Trattamenti)

Tali registri sono funzionali alla definizione delle misure di sicurezza dei trattamenti da adottare.

Essi contengono:

- gli estremi del **titolare e dei responsabili** del trattamento,
- **I dati** oggetto di trattamento
- le **finalità** del trattamento messe in atto dall'ente,
- una descrizione delle **categorie di interessati**,
- una descrizione delle **misure di sicurezza adottate**.

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

3. Valutazione d'Impatto (DATA PROTECTION IMPACT ASSESSMENT)

La valutazione d'impatto va a sostituire l'obbligo di notifica al garante del trattamento e deve essere messa in atto **quando il trattamento preveda RISCHI ELEVATI** (es. distruzione o perdita, anche accidentale, dei dati, accesso non autorizzato, trattamento non consentito, trattamento non conforme alle finalità della raccolta), **per i diritti degli interessati.**
Essa deve essere effettuata dal titolare, sentito il DPO, e deve contenere:

- la **descrizione** del trattamento;
- **le finalità** del trattamento;
- la **valutazione dei rischi** eventuali per gli interessati;
- i meccanismi per **garantire la protezione del dato**, in conformità con il Regolamento.

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

Ad essa si collegano le **MISURE DI SICUREZZA DA ADOTTARE** (ex art. 32 Regolamento). Tra esse:

- ✓ **Pseudonimizzazione e cifratura**
- ✓ **Capacità di assicurare in maniera permanente riservatezza, integrità, disponibilità e resilienza dei servizi di trattamento;**
- ✓ **Capacità di ripsristino rapido dell'accesso in caso di incidente fisico o tecnico**
- ✓ **Procedura per testare l'efficacia delle misure tecniche ed organizzative**

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

Definiamo un **livello di sicurezza *ADEGUATO*** quando si riesce a far fronte a rischi di:

- **DISTRUZIONE;**
- **PERDITA;**
- **MODIFICA;**
- **DIVULGAZIONE NON AUTORIZZATA;**
- **ACCESSO IN MODO ACCIDENTALE O ILLEGALE a dati trasmessi, conservati o comunque trattati.**

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

4. Violazione dei dati personali DATA BREACH

Per violazione dei dati personali (in seguito "**data breach**") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'ente.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati,
provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione sono i seguenti:

- **danni fisici, materiali o immateriali alle persone fisiche**
(si pensi al danno derivante da una diffusione non autorizzata di dati di carattere sanitario);

- **perdita del controllo dei dati personali**
(si pensi ad una perdita/distruzione di un data base ospedaliero contenente dati sanitari di minori ricoverati)

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

- **limitazione dei diritti, discriminazione**

(si pensi alla diffusione non autorizzata di dati relativi a problematiche sanitarie di minori in ambito scolastico);

- **furto o usurpazione d'identità;**

(si pensi alla violazione di data base delle pubbliche amministrazioni per le clonazioni di documenti di identità o furto di informazioni);

- **perdite finanziarie, danno economico o sociale**

(si pensi al danno derivante dalle clonazioni dei dati relativi alle carte di credito o, più in generale, di dati bancari);

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

- **decifratura non autorizzata della pseudonimizzazione**

(si pensi alla decifratura e diffusione di dati pseudonimizzati per graduatorie comunali di sussidi sociali a famiglie bisognose);

- **perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).**

(si pensi alla divulgazione di dati relativi allo stato di salute di un professionista, curato da un medico specialista)

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

I rischi per i diritti e le libertà degli interessati possono essere **considerati "elevati"** quando la violazione può, a titolo di esempio:

- **coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;**
- **riguardare categorie particolari di dati personali;**
- **comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);**

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

LE PRINCIPALI NOVITA' DEL NUOVO REGOLAMENTO

5. Nomina del Responsabile Protezione Dati (DPO) (ex art . 37 Reg.)

Identifica il ruolo aziendale che ha il compito di assicurare che le operazioni di trattamento dei dati personali avvengano in maniera lecita e nel rispetto della normativa vigente.

Egli deve essere sistematicamente designato **(vi è un obbligo di legge)** dal titolare o dal responsabile del trattamento:

- Quando il trattamento dei dati viene effettuato da un'***autorità pubblica***;
- Quando le attività del titolare consistono in trattamenti che richiedono il ***monitoraggio regolare e sistematico degli interessati su larga scala***;
- Quando le attività del titolare consistono nel ***trattamento su larga scala di dati sensibili o dati biometrici***
- *(come nella vecchia accezione)*, ai sensi dell'art. 9 del Regolamento stesso.

RUOLO DEL DATA PROTECTION OFFICER

La figura del Data Protection Officer si caratterizza per:

DIRITTI

- il diritto all'**indipendenza** nell'esercizio della funzione;
- il diritto al riconoscimento alla sua **autorevolezza**;
- il diritto di **non esclusività nei compiti attribuiti** (può svolgere altre ulteriori attività nello stesso contesto, ma può ricoprire incarichi aggiuntivi presso altri soggetti, qualora venisse designato con un contratto di servizi).

RUOLO DEL DATA PROTECTION OFFICER

OBBLIGHI

- deve **riferire criticità o problematiche rilevate** e relazionarsi direttamente con titolare e responsabile del trattamento;
- deve rendersi **disponibile nei confronti degli interessati** al trattamento, informandoli sui trattamenti ad essi riferibili e fugando ogni loro dubbio;
- è tenuto alla **massima riservatezza** nell'assolvimento dei compiti che attengono al suo incarico.

RUOLO DEL DATA PROTECTION OFFICER

COMPITI

- **informare e fornire consulenza** sugli obblighi previsti dal regolamento;
- **sorvegliare sull'osservanza del regolamento**, l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti;
- **fornire pareri**, se richiesto, **in merito alla valutazione d'impatto** e sorvegliarne lo svolgimento;
- svolgere attività di cooperazione e di **raccordo con l'autorità di controllo**;
- effettuare un'attenta **valutazione dei rischi** connessi all'attività di trattamento dei dati.

IL REGIME SANZIONATORIO

Sinteticamente:

- Sanzioni amministrative pecuniarie previste nel caso di mancato adempimento degli obblighi ai quali sono assoggettati TUTTI GLI ENTI, in qualità di **titolari del trattamento:**

FINO A 10 MLN DI EURO o FINO AL 2% DEL FATTURATO

- Sanzioni amministrative pecuniarie previste nel caso di **violazione dei diritti dell'interessato:**

FINO A 20 MLN DI EURO o FINO AL 4% DEL FATTURATO

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

In questa sezione andremo a riassumere quanto è stato disposto a carico degli autorizzati al trattamento (valido anche per i responsabili del trattamento da cui dipendono i dipendenti gerarchicamente sottoposti in tema di trattamento).

Più che di accorgimenti, si tratta di vere e proprie regole di condotta nel trattamento dei dati: il tutto a beneficio di chi materialmente tratta il dato e dell'ente, più in generale.

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'autorizzato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il ***rispetto delle misure di sicurezza***, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

- le singole fasi di lavoro e la condotta da osservare devono consentire di ***evitare che i dati*** siano soggetti a ***rischi di perdita o distruzione***, che vi possano accedere ***persone non autorizzate***, che vengano svolte operazioni di ***trattamento non consentite o non conformi*** ai fini per i quali i dati stessi sono stati raccolti;

- in caso di ***allontanamento,*** anche temporaneo, ***dalla propria postazione di lavoro*** si devono porre in essere tutte le misure necessarie affinché soggetti terzi, anche se dipendenti***, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo sia automatizzato;***

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

- ***non devono essere eseguite operazioni di trattamento per fini non previsti*** tra i compiti assegnati dal responsabile del trattamento, ben delineati nel registro/mappature delle attività di trattamento consegnato all'autorizzato

- devono essere svolte ***le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti***;

- deve essere costantemente verificata ***l'esattezza*** dei dati trattati e ***la pertinenza*** rispetto alle finalità perseguite nei singoli casi.

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

- ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

Uso esclusivo per attività lavorativa, riservatezza e custodia di dati di soggetti interessati;

- GESTIONE DELLE PASSWORD

Modifica alla scadenza (lettere, numeri, maiuscolo), no diffusione a terzi

- ANTIVIRUS

Controllo aggiornamento antivirus e firewall e massima attenzione nello scaricare files che potrebbero compromettere l'integrità del sistema informatico (contenitore di dati);

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

- SALVATAGGIO DEI DATI

Salvataggio su server (no pc locale); divieto di eseguire copie su supporti esterni

- PROTEZIONE DEI SISTEMI INFORMATICI PORTATILI

(computer portatile, smartphone, palmari o tablet dell'Ente)

Adozione di sistemi di custodia e conservazione idonei; operare sempre nella massima riservatezza.

- USO DI INTERNET E POSTA ELETTRONICA

Utilizzo esclusivo per le mansioni assegnate e solo per informazioni dell'ente; utilizzo esclusivo di software dell'ente; divieto di scaricare files estranei all'utilizzo per conto dell'ente;

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION

- TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Assicurarsi sempre del destinatario ricevente nelle comunicazioni o trasmissioni di dati e documenti; distruzione fisica del documento al termine del trattamento.

- ARCHIVI CARTACEI

I documenti devono essere custoditi con perizia; in caso di dati sensibili devono essere custoditi in stanze e/o armadi chiusi a chiave; l'accesso deve essere consentito solo agli autorizz*ati*

CODICE DI CONDOTTA PER LA CORRETTA GESTIONE DELLA DATA PROTECTION NELL'ENTE LOCALE

- ACCESSO AI DATI DELL'UTENTE

Accesso del Responsabile del Trattamento o Amministratore di Sistema esclusivamente per motivi di sicurezza informatica, assistenza tecnica manutentivi. In caso di prolungata assenza dell'utente si accederà ugualmente: al rientro le password di accesso saranno modificate.

- USO DEL CELLULARE PRIVATO DURANTE IL PERIODO DI LAVORO

Vietato, salvo deroghe valutate caso per caso.

- CONTROLLI DA PARTE DELLA TITOLARITA'

Controllo del titolare del trattamento al fine di evitare condotte illecite nel trattamento

STEP DA SEGUIRE PER UNA CORRETTA GESTIONE DELLA DATA PROTECTION

- **Analisi struttura organizzativa dell'ente** con individuazione del titolare, dei responsabili e degli incaricati al trattamento;
- **Definizione, formalizzazione ed implementazione dei processi** (accountability/valutazione d'impatto/analisi dei rischi con conseguente adozione delle relative misure di sicurezza tecnico-organizzative/data breach);
- **Rielaborazione della documentazione in essere ALLA LUCE DEL NUOVO GDPR**;
- **Definizione di un sistema di controllo interno (sistema di deleghe);**
- **Formazione specifica del personale e dei soggetti coinvolti** (tipologie di dati trattati, valutazione d'impatto, misure di sicurezza, flusso dei processi);
- **Scelta e nomina DPO** (obbligatorio per il comune), **con adozione del Registro del trattamento** (obbligatorio per il titolare) **e Registro delle categorie di attività** (dei Responsabili del trattamento), o, in alternativa, **Registro Unico dei Trattamenti**.

IL DLGS 101/2018 –Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 - NUOVO CODICE PRIVACY

Il decreto legislativo numero 101 del 10 agosto 2018 è stato pubblicato nella Gazzetta Ufficiale dello scorso 4 settembre e, con esso, la normativa nazionale in materia di privacy si è adeguata alle disposizioni del Gdpr.

Quanto in esso previsto è entrato in vigore dal 19 settembre 2018.

Di seguito andremo a sintetizzare le principali novità introdotte dal decreto.

Sanzioni penali: reclusione da sei mesi fino a sei anni

- **Trattamento illecito di dati**: "Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione del Regolamento arreca un danno all'interessato, è punito con la reclusione da sei mesi fino a un anno e sei mesi. E nei casi più gravi fino a tre anni.

- **L'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala** è punita con la reclusione da uno a quattro anni.

- **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala** è punita con la reclusione da uno a sei anni.

- **L'inosservanza dei provvedimenti del Garante** è punita con la reclusione da tre mesi a due anni.

Sanzioni amministrative

Sarà compito del Garante Privacy scrivere le regole per l'applicazione delle sanzioni amministrative.

"Per i primi 8 mesi dalla data di entrata in vigore del presente decreto", si legge nell'articolo 22, comma 13, "il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento Ue, della fase di prima applicazione delle disposizioni sanzionatorie", ma non significa che non potrà irrogare le sanzioni amministrative che possono essere elevate.

Sanzioni amministrative di minore e maggiore entità

Le sanzioni amministrative pecuniarie di minore entità possono raggiungere i 10 milioni di euro per i singoli e per le imprese fino al 2% del fatturato globale annuo se superiore e riguardano le violazioni degli obblighi per:

Il titolare ed il responsabile del trattamento
L'organismo di certificazione.
l'organismo di controllo dei codici di condotta.

Le sanzioni amministrative pecuniarie di maggiore entità possono arrivare a 20 milioni di euro per i singoli o fino al 4% del fatturato mondiale annuo per le aziende, a prescindere da dove sia la sede principale, che può essere anche fuori dall'Europa, nel caso di violazioni dei diritti dell'interessato (es. trattamento illecito dei dati).

Modalità semplificate di adempimento degli obblighi per le Pmi

Il testo del nuovo provvedimento prende in particolare considerazione le esigenze di semplificazione delle micro, piccole e medie imprese, affidando al Garante per la protezione dei dati personali il compito di promuovere delle modalità semplificate di adempimento degli obblighi di trattamento, nel rispetto delle disposizioni del Gdpr e del nuovo codice privacy

Curriculum vitae

Il d.lgs. 101/2018 stabilisce che l'informativa ex art. 13 GDPR vada fornita al momento del **"primo contatto utile", successivo all'invio del curriculum.** Nei limiti delle finalità stabilite dall'articolo 6, paragrafo 1) lettera b) del Regolamento UE, il consenso del candidato al trattamento dei dati personali contenuti nel curriculum non è richiesto.

Minori sui social da 14 anni senza l'ok dei genitori

In Italia dal 19 settembre chi ha 14 anni potrà iscriversi liberamente sui social network e utilizzare i servizi di messaggistica istantanea (WhatsApp, ecc.). Questa è un'altra novità contenuta del testo del decreto di adeguamento al Gdpr. Gli under 14 hanno bisogno del consenso di chi esercita la responsabilità genitoriale.

Dati biometrici

Il decreto dà il via libera al trattamento dei dati genetici, biometrici e relativi alla salute, che dovrà avvenire seguendo le misure di garanzia disposte dal Garante Privacy.

Ci sono novità a seguito del Decreto Legislativo n. 101 in materia di Informativa Privacy e consenso al trattamento dei dati personali?

Nessuna novità.

Per l'Informativa Privacy continuano a valere tutte le regole dettate dagli articoli 13 e 14 del GDPR. Stesso discorso per il consenso al trattamento dei dati personali, ove continuano a valere, come regole generali, quelle previste dall'art. 6, comma 1, lett. *a)*, e dall'art. 7 del GDPR.

Garante Privacy

Il nuovo codice privacy rafforza i poteri e aumenta i compiti del Garante Privacy, per il quale il legislatore ha stabilito per il personale **il limite di 162 unità**. Novità anche per chi desidera diventare componente dell'Autorità:

"Il Collegio è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti devono essere eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante almeno sessanta giorni prima della nomina. Le candidature devono pervenire almeno trenta giorni prima della nomina e i curricula devono essere pubblicati negli stessi siti internet".

Infine è cambiata anche la forma di tutela garantita a chi crede di aver subìto una violazione della privacy: **non più il ricorso, ma l'interessato può proporre un reclamo al Garante Privacy oppure rivolgersi all'autorità giudiziaria**.

Dati per la ricerca scientifica e per fini statistici

L'Autorità Garante per la protezione dei dati personali dovrà anche promuovere regole deontologiche per il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici che può essere effettuato, ecco la novità introdotta, anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

Giustizia

Tutti gli organi giudiziari sono obbligati a nominare il Data Protection Officer (**Dpo**).

Persone decedute

I dati personali delle persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

Cosa accade adesso per tutti quei provvedimenti emanati dal Garante per la protezione dei dati personali antecedenti al 25 maggio 2018 ?

A decorrere dal 25 maggio 2018, tutti i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il GDPR e con le disposizioni del nuovo Codice Privacy.

Discorso leggermente differente, invece, deve essere fatto per le autorizzazioni generali, per le quali il Garante dovrà pronunciarsi sulla loro compatibilità con il nuovo impianto normativo – ed eventualmente aggiornarle – entro 90 giorni dalla data di entrata in vigore del Decreto Legislativo 101.

Procedimenti pendenti

Il decreto legislativo consente la definizione agevolata dei procedimenti pendenti relativi a violazioni amministrative del 'vecchio' codice Privacy, con il pagamento di una favorevole oblazione.

Ci sono 90 giorni per pagare la sanzione ridotta per le contestazioni pendenti. Si possono regolare le questioni **versando i 2/5 del minino edittale.**

La scadenza per il pagamento dell'importo è fissata al novantesimo giorno dall'entrata in vigore del decreto legislativo 101/2018.

GLI OBBLIGHI PER L'INGEGNERE

Occorre fare una puntualizzazione iniziale sui soggetti interessati dalla evoluzione normativa:

1. **Ingegnere lavoratore dipendente;**

2. **Ingegnere libero professionista;**

3. **Società di ingegneria.**

Ingegnere lavoratore dipendente

Per questa tipologia di professionista **non vi sono obblighi diretti in capo alla persona**: ci sono delle responsabilità derivanti dalla posizione ricoperta nell'ente datore di lavoro.

- **Ente pubblico**: l'ingegnere potrebbe essere individuato come responsabile o autorizzato al trattamento, a seconda della collocazione della sua posizione organizzativa nel regolamento degli uffici o dei servizi dell'ente

- **Azienda privata**: l'ingegnere potrebbe essere individuato come responsabile o autorizzato al trattamento, a seconda della collocazione nell'organigramma aziendale.

Se ricopre il ruolo, **non da dipendente**, di **amministratore unico/amministratore delegato/presidente di CDA, ai fini della protezione dati personali risulta TITOLARE DEL TRATTAMENTO**

Ingegnere libero professionista

In questo caso la nuova normativa dispone che il professionista rispetti queste prescrizioni nella propria attività:

1. Osservanza dei principi del trattamento e tutela dei diritti dell'interessato.

2. Registro dei trattamenti.

3. Misure di sicurezza per il trattamento.

4. Informative a corredo dei contratti e consensi sottoscritti.

1. **Osservanza dei principi del trattamento e tutela dei diritti dell'interessato.**

Principi del trattamento

- LICEITÀ
- CORRETTEZZA
- TRASPARENZA
- LIMITAZIONE DELLE FINALITA'
- MINIMIZZAZIONE DEI DATI
- ESATTEZZA
- LIMITAZIONE DELLA CONSERVAZIONE
- INTEGRITA' E RISERVATEZZA

DIRITTI DEGLI INTERESSATI

DIRITTO DI ACCESSO (ex art. 15 GDPR)

DIRITTO DI RETTIFICA (EX ART. 16 GDPR)

DIRITTO ALLA CANCELLAZIONE (C.D. DIRITTO ALL'OBLIO) (EX ART. 17 GDPR)

DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO (EX ART.18 GDPR)

DIRITTO ALLA PORTABILITA' DEI DATI (EX ART. 20 GDPR)

DIRITTO DI OPPOSIZIONE (EX ART. 21 GDPR)

2. Registro dei trattamenti.

Tali registri sono funzionali alla definizione delle misure di sicurezza dei trattamenti da adottare.

Essi contengono:

- gli estremi del titolare e dei responsabili del trattamento,
- I dati oggetto di trattamento
- le finalità del trattamento
- una descrizione delle categorie di interessati,
- una descrizione delle misure di sicurezza adottate
- Le categorie di destinatari.

3. Misure di sicurezza per il trattamento.

la pseudonimizzazione e la cifratura dei dati personali

la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

INFORMATIVA

Elementi da fornire all'interessato:

- **Dati del Titolare del trattamento;**
- **Dati del DPO (se presente);**
- **Finalità del trattamento;**
- **Destinatari dei dati trattati;**
- **Periodo di conservazione dei dati e/o durata del trattamento;**
- **Se vi è una finalità ulteriore rispetto a quella originaria, ne deve essere data informazione all'interessato.**

CONSENSO AL TRATTAMENTO

MANIFESTAZIONE DI VOLONTÀ da parte dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva al trattamento dei dati personali che lo riguardano che sia:

Libera, (senza condizionamenti)
Specifica, (relativa esclusivamente al trattamento che si deve mettere in atto)
Informata (che evidenzia conoscenza diretta del trattamento)
Inequivocabile (che esclude qualsiasi riserva o incertezza),

SOCIETA' DI INGEGNERIA

ESSE VENGONO TRATTATE A LIVELLO DI DATA PROTECTION COME TUTTE LE AZIENDE

In sostanza, a ciò che deve osservare il singolo professionista vanno aggiunte:

- La nomina del DPO (ove prescritto dalla legge);
- L'adozione di un REGOLAMENTO INTERNO e dei CODICI DI CONDOTTA per responsabili ed incaricati al trattamento: questi ultimi non sono obbligatori, ma fortemente consigliabili.

GRAZIE PER L'ATTENZIONE