LEGGE SULLA TUTELA DELLA PRIVACY

Dal D.Lgs. 30-06-2003, n. 196

Codice in materia di protezione dei dati personali

al

GDPR

Aggiornato in base ai seguenti provvedimenti:

- • decreto legislativo 14 settembre 2015, n. 151.
- • decreto legge 18 febbraio 2015, n. 7,
  convertito, con modificazioni, dalla Legge 17 aprile 2015, n. 43;
- • legge 27 dicembre 2013, n. 147;
- • decreto legislativo 14 marzo 2013, n. 33;
- • decreto legislativo 28 maggio 2012, n. 69;
- • decreto legge 9 febbraio 2012, n. 5,
  convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35;
- • decreto legge 6 dicembre 2011, n. 201,
  convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
- • decreto legge 13 maggio 2011, n. 70
  convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
- • legge 4 novembre 2010, n. 183;
- • legge 29 luglio 2010, n. 120;
- • decreto-legge del 25 settembre 2009, n. 135
  convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
- • legge 4 marzo 2009, n. 15;
- • decreto-legge del 30 dicembre 2008, n. 207
  convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
- • decreto-legge 25 giugno 2008, n. 112
  convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
- • decreto legislativo 30 maggio 2008, n. 109;
- • legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- • decreto-legge 28 dicembre 2006, n. 300
  convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
- • decreto-legge 12 maggio 2006, n. 173
  convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
- • decreto-legge 30 dicembre 2005, n. 273
  convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
- • decreto legge 30 novembre 2005, n. 245
  convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;
- • decreto legislativo 7 settembre 2005, n. 209;
- • decreto-legge 27 luglio 2005, n. 144
  convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
- • decreto-legge 30 dicembre 2004, n. 314
  convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;
- • decreto-legge 9 novembre 2004, n. 66
  convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;
- • decreto-legge 24 giugno 2004, n. 158
  convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;
- • decreto-legge 29 marzo 2004, n. 81
  convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;
- • decreto legislativo 22 gennaio 2004, n. 42;
- • decreto-legge 24 dicembre 2003, n. 354
  convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45

Obiettivo

Le finalità del d. lgs. 196/03 consistono nel riconoscimento del diritto del singolo sui **propri dati personali** e nella disciplina delle diverse operazioni di gestione (tecnicamente “**trattamento**") dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi.

Lo scopo della legge non è quello di impedire il trattamento dei dati, ma di evitare che questo avvenga contro la volontà dell‘avente diritto ovvero secondo modalità pregiudizievoli.

Diritto alla protezione dei dati personali

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto ad una funzione pubblica e la relativa valutazione non sono oggetto di protezione della riservatezza personale

Finalità

1. Il presente testo unico, di seguito denominato «codice», garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati

Principio di necessità nel trattamento dei dati

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

Alcune definizioni

Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato

Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale

Dati giudiziari

I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato

Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

Ha facoltà di conoscere: quali dati vengono trattati, come e con quali fini avviene il trattamento, l'autore del trattamento, i soggetti a cui detti dati possono essere comunicati.

In ragione del diritto di accesso l'interessato può poi chiedere che i dati da altri detenuti corrispondano al vero, pretendendone l'aggiornamento o la cancellazione a seconda dei casi. Se poi i dati sono trattati in maniera difforme dalla legge, l'interessato può chiedere la cancellazione degli stessi o il blocco del trattamento.

Titolare

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza

Responsabile

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

Banca di dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti

Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Misure minime

il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31

31. Obblighi di sicurezza

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Garante

Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

Garante - Presidente

I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive

All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

Compiti del garante

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico

b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;

c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti

d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

e) promuovere la sottoscrizione di codici

f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti anche a seguito dell'evoluzione del settore;

g) esprimere pareri nei casi previsti;

h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati

i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

l) tenere il registro dei trattamenti

m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Diritto di accesso ai dati personali ed altri diritti

L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

Diritto di accesso ai dati personali ed altri diritti

L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Divieti di comunicazione e diffusione

1. *La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:*

a) *in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e)* (*conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*);

b) *per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.*

2. *È fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati*

Tutela dei diritti

Chi sia leso nei diritti sui propri dati riconosciuti dal d. lgs. 196/03 (raccolta dei dati senza il consenso, consenso acquisito senza fornire la preventiva informativa sulla legge, trattamento dei dati oltre i limiti del consenso dato, negazione o limitazione al diritto di accesso) può ricorrere al Garante per la protezione dei dati personali (con una procedura piuttosto rapida e costi contenuti) o al giudice civile (con costi e tempi maggiori). Se invece a seguito del trattamento dei dati non conforme alla legge si è subito un danno (non necessariamente economico, dunque anche consistente nel disagio arrecato dal fatto) il risarcimento può essere concesso solamente dal giudice civile.

Risarcimento del danno

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile (Responsabilità per l'esercizio di attività pericolose : *"Chiunque cagiona danno ad altri nello svolgimento di un'attività, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno"* → inversione dell'onere della prova, il danneggiante deve dimostrare che ha fatto tutto il possibile per evitare il danno, il quale però evidentemente si è verificato!) Questo riferimento all'art. 2050 del c.c. viene considerato da alcuni eccessivo ma formalmente si tratta di un riferimento ineccepibile (esiste la possibilità di un danno e questo è quantificabile).

Privacy e amministrazioni

L'amministrazione titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza si assicura il rispetto di quanto previsto in merito al:

- principio di necessità nel trattamento dei dati;
- diritto di accesso ai dati personali da parte dell'interessato;
- alle modalità del trattamento e ai requisiti dei dati;
- all'informativa da fornire agli interessati;
- alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- alle misure minime di sicurezza.

Adempimenti ordinari per le imprese

Le imprese si caratterizzano per una grande quantità di dati trattati ma generalmente riconducibili a poche e ben determinabili tipologie.

nella maggior parte dei casi vi sarà trattamento di dati personali comuni di clienti/ fornitori per la gestione delle attività di fatturazione e registrazione contabile.

Trattamento dati sensibili nelle imprese

L'ipotesi più frequente di trattamento di dati sensibili per tali soggetti può essere rappresentata dalla gestione interna del personale dipendente o se si conservino ed utilizzino e CV di aspiranti lavoratori per assunzioni dirette

Tipologia di atti e documenti trattati

- Questa categoria si troverà a elaborare una vasta serie di documenti contenenti dati personali e/o sensibili:
- Fatture, contratti, parcelle
- Preventivi/ progetti
- Bilanci ed elaborazioni contabili
- Pratiche amministrative

Tipologia di atti e documenti da trattare come dati sensibili

- Fotocopie di documenti personali
- Documenti relativi al personale dipendente
- Certificati medici dei dipendenti/assicurati
- Schede notizie relative alla clientela (assicurazioni, banche)
- Curriculum vitae

Tipologie di dati

Le documentazioni conterranno dati:

- COMUNI (dati anagrafici, residenza, domicili fiscali, elementi patrimoniali, riproduzioni fotografiche, incarichi professionali, ecc.)
- SENSIBILI/ GIUDIZIARI (stato di salute, presenza di handicap, sentenze/ provvedimenti giudiziari e amministrativi).

Adempimenti minimi

Le imprese che trattano dati comuni o sensibili hanno l'obbligo di porre in essere una serie di adempimenti differenziati in base alla struttura aziendale e alla natura dei dati trattati.

Adempimenti minimi per dati comuni

DOCUMENTALI

- Gli adempimenti di tipo documentale sono rappresentati da moduli cartacei, sottoscritti all'occorrenza dal soggetto coinvolto.
- Anche per i documenti cartacei è necessario porre in essere le misure di sicurezza previste del Codice della privacy (conservazione in luoghi idonei e inaccessibili alla generalità delle persone non autorizzate)

informativa

Tutti i soggetti, quali di un trattamento di dati, dovranno adempiere all'obbligo di informare l'interessato.

Come per le ditte individuali e le piccole imprese anche le strutture più organizzate sono tenute al rilascio di un'informativa, nei confronti di:

- Clienti e fornitori di ogni natura
- Dipendenti e collaboratori

Adempimenti minimi per dati sensibili/giudiziari

L'utilizzo di dati sensibili o giudiziari nello svolgimento dell'attività, impone al titolare ulteriori adempimenti e cautele: un utilizzo scorretto di tali dati può arrecare danno al soggetto interessato.

Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati siano resi disponibili, integri e riservati.
- I dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito.

COSA CAMBIA CON LA GDPR???

GDPR

GDPR (General Data Protection Rules) è il nuovo Regolamento dell'Unione Europea in materia di privacy entrato in vigore il 25 maggio 2018.

L'Italia ha promulgato un decreto di adeguamento della legge sulla Privacy al GDPR

COSA SI INTENDE PER REGOLAMENTO?

Il regolamento è uno degli atti legislativi dell'Unione europea, insieme a direttive e decisioni.

Si caratterizza per avere:

- portata generale (vale in tutti i paesi)
- applicabilità diretta in tutti i suoi elementi (diventa legge subito, senza dover passare per il recepimento da parte degli Stati membri).

I paesi possono decidere di rivedere la propria legislazione se si creano incompatibilità evidenti con le nuove regole europee. Nel caso dell'Italia, ad esempio, si è abolita la parte generale del vecchio Codice della privacy (a sua volta ispirato a una direttiva risalente al 1995) e si sono diluite le restanti norme in un decreto.

SCOPI DELLA GDPR

Questo nuovo Regolamento nasce dalle esigenze di **certezza giuridica, armonizzazione** e **maggiore semplicità** delle norme riguardanti il trasferimento di dati personali dall'UE verso altre parti del mondo.

Serve inoltre a rispondere alle nuove esigenze nate dagli sviluppi tecnologici.

A CHI SI APPLICA?

Le norme si applicano anche alle imprese situate al di fuori dell'UE che offrono servizi o prodotti all'interno del mercato UE.

Tutte le aziende, ovunque stabilite, dovranno rispettare le nuove regole.

Imprese ed enti avranno più responsabilità e in caso di inosservanza delle regole rischiano pesanti sanzioni.

SPORTELLO UNICO (ONE STOP SHOP)

Il GDPR ha introdotto anche uno sportello unico che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.

Le imprese che operano in più stati UE potranno rivolgersi al Garante del paese in cui hanno la sede principale

IMPATTO SULLE AZIENDE

L’impatto è molto forte poiché la Gdpr riguarda le aziende che gestiscono qualsiasi tipo di dato personale. Dalle informazioni sui propri dipendenti alla profilatura dei clienti per conto terzi: «La Gdpr coinvolge tutte le aziende che trattano dati Il che può significare le informazioni in mano alle risorse umane sul proprio organico o l’analisi di dati per attività di marketing “targettizzato”, mirato su misura a seconda del cliente».

PRINCIPALI ADEMPIMENTI

- Nomina del **DPO** (responsabile della protezione dati)
- Controlli sulle misure previste in caso di **data breach** (tutti i casi in cui si verifica una perdita accidentale di dati come furto di un pc o di un hardisk ad esempio)
- **Registro dei trattamenti**

DPO (Data Protection Officer)

Il responsabile della protezione dei dati deve gestire i dati raccolti dall'azienda nel rispetto della normativa sulla privacy

Il DPO può essere nominato internamente o esternamente all'azienda

Il DPO deve avere una specifica competenza "della normativa e delle prassi in materia di dati personali nonché delle norme e delle procedure amministrative che caratterizzano il settore".

Funge da punto di contatto tra l'ente/azienda e il garante.

DPO (Data Protection Officer)

- E’ importante che il DPO abbia l’autonomia decisionale e sia estraneo rispetto alla determinazione delle finalità e delle modalità del trattamento dei dati se si vuole restituire agli interessati quella sovranità sulla circolazione dei propri dati.
- Riferisce direttamente al vertice
- È indipendente, non riceve istruzioni per quanto riguarda l’esecuzione dei compiti
- Gli vengono attribuite risorse umane e finanziarie adeguate alla mission.

QUANDO SERVE UN DPO?

L'istituzione di questa figura è necessaria quando:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali
- Quando le attività principali del titolare del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.
- Quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari/dati sensibili) o dati relativi a condanne penali e a reati

REGISTRO DEI TRATTAMENTI

- L'obbligo di tenuta del registro riguarda tutti i titolari e responsabili del trattamento dei dati personali (eccetto PMI con meno di 250 dipendenti). L'obbligo si estende anche alle PMI quando dal trattamento dei dati può derivare un rischio per i diritti e le libertà dell'interessato, qualora il trattamento non sia occasionale o se riguardi particolari tipologie di dati.
- All'interno del registro dei trattamenti bisognerà indicare le caratteristiche del titolare del trattamento e del responsabile del trattamento.
- Potrà essere utilizzato a fini di controllo
- Serve come strumento di controllo delle attività poste in essere

PRINCIPALI CAMBIAMENTI

In sintesi estrema il GDPR:

- Introduce regole più chiare su informativa e consenso
- Definisce i limiti al trattamento automatizzato dei dati personali
- Pone le basi per l'esercizio di nuovi diritti
- Stabilisce criteri rigorosi per il trasferimento degli stessi diritti al di fuori dell'UE
- Fissa norme rigorose per i casi di violazione dei dati

INFORMATIVA

- Tra le principali novità del nuovo regolamento ci sono le nuove regole in materia di informativa e consenso:
- Dovrà essere chiara e semplice con un linguaggio di facile comprensione (facendo anche uso di icone se ritenuto opportuno)
- Si dovrà indicare come saranno utilizzati i dati e per quanto tempo verranno conservati nei data base.
- Se i dati saranno raccolti con finalità di marketing o condivisi con altre aziende si dovrà indicare in maniera esplicita ai soggetti che i propri dati potrebbero essere trasferiti a terzi per finalità di marketing. In caso di mancanza di esplicito consenso i dati non potranno essere comunicati.

CONSENSO

Il consenso al trattamento dei dati personali dovrà essere preventivo e inequivocabile, così come previsto già oggi. Quello che cambia è la modalità per esprimerlo: non varrà mai la regola che chi tace acconsente, il consenso dovrà essere esplicito e mai basato ponendo all'interessato una serie di opzioni già selezionate.

Se l'azienda, negli anni precedenti, ha raccolto il consenso dei propri clienti utilizzando caselle precompilate dovrà chiedere ai clienti (che già avevano dato il consenso) l'autorizzazione al trattamento dei dati utilizzando le nuove modalità previste dal GDPR.

REVOCA DEL CONSENSO

Il consumatore potrà revocare il consenso in ogni momento.

Chi detiene i dati sarà obbligato a cancellarli tutti.

CONSENSO PER I MINORENNI

Il GDPR prevede modifiche anche riguardo il consenso da parte di minori per la fruizione di servizi su internet e social media: per i minori di 16 anni dovranno dare il consenso i genitori o chi esercita la potestà genitoriale.

PORTABILITÁ DEI DATI

I consumatori possono richiedere il trasferimento dei propri dati personali da un titolare del trattamento ad un altro.

Ad esempio è possibile cambiare il provider di posta elettronica senza perdere i contatti e i messaggi salvati o, allo stesso modo, cambiare il gestore dell'energia.

DIRITTO ALL'OBLIO E CONSERVAZIONE LIMITATA

Sulla base del diritto all'oblio il consumatore può richiedere la cancellazione dei propri dati personali online nei casi in cui i dati sono trattati solo sulla base del consenso, se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti, se i dati sono trattati illecitamente o se l'interessato si oppone legittimamente al trattamento.

Es.: Richiesta di cancellazione di un articolo pubblicato su internet

DIRITTO ALL'OBLIO E CONSERVAZIONE LIMITATA

La conservazione dei dati dell'utente/cliente non potrà essere illimitata. La durata del trattamento deve essere collegata alla finalità per la quale è stato richiesto il consenso.

Ad esempio il consenso al trattamento dei dati relativi a un CV trasmesso potrà essere conservato per un periodo proporzionato all'attività di ricerca del personale nel medio e lungo termine.

ESCLUSIONE DEL DIRITTO ALL'OBLIO

Il diritto all'oblio è escluso qualora si tratti di informazioni di interesse generale o necessari per finalità storiche, statistiche o scientifiche.

VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

- In caso di violazione dei dati personali l titolare del trattamento è tenuto a darne comunicazione al Garante.
- Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

AUTORITÀ DI CONTROLLO

All’autorità di controllo, il nostro Garante Privacy, sono conferiti poteri di indagine, correttivi, autorizzativi e consultivi, oltre al potere di infliggere sanzioni amministrative pecuniarie.

PROFILO SANZIONATORIO

- Il GDPR stabilisce soltanto le sanzioni massime applicabili ad imprese e professionisti.
- In caso di mancato adempimento degli obblighi previsti le sanzioni saranno ispirate ai principi di **effettività, proporzionalità e dissuasività**.
- Le sanzioni saranno applicate dal Garante sulla base degli elementi raccolti nelle ispezioni e potranno arrivare fino a un massimo di **20 milioni di euro o al 4% del fatturato annuo.**

… L’UDIENZA È TOLTA!!!