Speciale
Privacy e GDPR

Confartigianato
Imprese Sud Sardegna

Come sopravvivere alla Privacy e all'Europa

begapps
comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale **è un diritto fondamentale**.

È opportuno che la protezione prevista dal presente regolamento si applichi alle **persone fisiche**, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi **senza una connessione con un'attività commerciale o professionale**. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività.

Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Ai fini del presente regolamento s'intende per:

1) **«dato personale»**: 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 a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)

2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di 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;

3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

7) **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

10)**«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11)**«consenso dell'interessato»**: qualsiasi manifestazione di volontà **libera, specifica, informata** e **inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

12)**«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (C85)

13)**«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

14) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)

15)**«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Alcune definizioni

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40)

a) l'interessato **ha espresso il consenso** al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43)

b) il trattamento **è necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44)

c) il trattamento **è necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento; (C45)

d) il trattamento **è necessario per la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica; (C46)

e) il trattamento **è necessario per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)

f) il trattamento **è necessario per il perseguimento del legittimo interesse del titolare del trattamento** o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47-C50)

Cosa prevede la GDPR?

GDPR:
General Data Protection Regulation
regolamento generale sulla protezione dei dati

La GDPR, è un testo che prova a uniformare le leggi europee sul trattamento dati e il (nostro) diritto a essere in pieno controllo delle informazioni che ci riguardano.

Il regolamento si compone di 99 articoli e istituisce alcune novità come il **diritto all'oblio** (gli utenti possono chiedere di rimuovere informazioni a proprio riguardo), la «**portabilità**» dei dati (si possono scaricare e trasferire dati da una piattaforma all'altra, senza vincolarsi a un certo account) e l'**obbligo di notifica in caso di data breach** (le aziende, se subiscono fughe di informazioni sensibili, devono comunicarlo entro 72 ore).

I destinatari sono i «**titolari del trattamento**», ossia chi gestisce le informazioni: privati e, soprattutto, aziende.

Confartigianato
Imprese Sud Sardegna

begapps
comunicazione

Quale sarebbe l'impatto su un'azienda "normale"?

L'impatto è più ampio di quanto si possa pensare, perché 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».

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Quali sono i principali obblighi?

Fra gli obblighi da tenere in considerazione:

- una richiesta di **consenso** in forma chiara (articolo 7);

- l'istituzione di un **registro delle attività** (articolo 30);

la **notifica delle violazioni** entro 72 ore (articolo 33);

la designazione di un «**responsabile protezione dati**» (articolo 37).

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Quali sono i principali obblighi?

Richiesta di **consenso** in forma chiara (articolo 7):

Per quanto riguarda il consenso, l'azienda deve chiedere il via **libera** «in modo chiaramente **distinguibile** dalle altre materie, in forma **comprensibile** e facilmente **accessibile**, utilizzando un linguaggio semplice e chiaro (al contrario delle vecchie e chilometriche informative)».

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Quali sono i principali obblighi?

Istituzione di un **registro delle attività** (articolo 30):

Si obbligano i titolari a dotarsi di un registro delle attività dove si elencano - tra le altre cose - le finalità dell'elaborazione dei dati, i destinatari, l'eventuale scadenza per la loro cancellazione.

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con **meno di 250 dipendenti** ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Quali sono i principali obblighi?

Cosa è il Data Breach:
I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

Notifica delle violazioni entro 72 ore (articolo 33):

In caso di **data breach**, la violazione dei propri dati, scattano obblighi di notifica alle autorità molto più stringenti:

il titolare deve comunicare l'accaduto «entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche».

Confartigianato Imprese Sud Sardegna

begapps comunicazione

Quali sono i principali obblighi?

Designazione di un «**responsabile protezione dati**» (articolo 37):

Infine si va a istituzionalizzare su scala EU una figura già accolta da alcune legislazioni:

il **data protection officer - DPO**, assunto tra i dipendenti dell'azienda o presso una società esterna con il ruolo di vigilare sull'applicazione effettiva della GDPR da parte del suo titolare.

Confartigianato Imprese Sud Sardegna

begapps comunicazione

E se si viola il regolamento?

A seconda della gravità dell'infrazione, le multe sono divise in due scaglioni:

fino a un massimo di 10 milioni di euro o, per le imprese, il 2% del fatturato (se superiore);

oppure **fino a** un massimo di 20 milioni o il 4% del turnover, sempre per le aziende e sempre in rapporto al giro d'affari.

Per farsi un'idea, il Garante alla privacy è riuscito a incassare nel 2015 poco più di 3,3 milioni di sanzioni.

La multa più "leggera" (10 milioni o 2% turnover) viene inflitta per la trasgressione di principi come la privacy by design (mancata protezione dei dati fin dalla progettazione) o la carenza di misure adatte a garantire un buon standard di sicurezza.

Quella più pesante (20 milioni o 4% del turnover) arriva in caso di violazione dei principi fondamentali, come la negazione del diritto all'oblio o l'opacità nella richiesta di consenso dei dati.

Non è previsto un periodo di “tolleranza” di sei mesi?

Non è chiaro.

Il Garante alla privacy, dovrebbe allinearsi alla posizione già intrapresa dal suo omologo francese (Commission nationale de l'informatique et des libertés) e consentire una specie di stand-by di sei mesi, dove le aziende ritardatarie possono evitare sanzioni.

Ma l’impresa deve comunque mostrare di avere avviato un piano di adeguamento ed essere consapevole delle priorità per rientrare nel perimetro del regolamento.

Sul sito però il Garante ha smentito:

Gdpr, Garante privacy: nessuna pronuncia su differimento applicazione sanzioni

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8469593

Buon lavoro!

Confartigianato
Imprese Sud Sardegna

begapps
comunicazione