DATA PROTECTION & SECURITY

Novità e azioni per essere GDPR Ready

brennercom

IL NUOVO REGOLAMENTO EUROPEO - GDPR

brennercom
DATA PROTECTION & SECURITY

Il GDPR, «**General Data Protection Regulation**», rappresenta il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, entrato in vigore il 25 maggio 2016 ed interamente applicabile il 25 maggio 2018.

Art.83 GDPR: le sanzioni amministrative, a seconda delle circostanze possono essere fino a 20 milioni di euro o fino al 4% del fatturato

GDPR & DIGITALIZZAZIONE

brennercom

DATA PROTECTION & SECURITY

Uno degli elementi caratterizzanti la trasformazione digitale è la possibilità di raccogliere, analizzare e rendere fruibile l'enorme quantità di dati, anche personali e particolari, derivanti dalla digitalizzazione.

Il regolamento GDPR, **pienamente in vigore** dal **25 maggio 2018**, interviene responsabilizzando le aziende che trattano questi dati, definendo nuovi diritti per le persone, nuove figure di garanzia e nuovi obblighi.

Il testo, nell'affrontare il delicato tema dell'esportazione dei dati personali al di fuori dell'Europa, chiama nel merito il settore del **cloud computing** coinvolgendolo pienamente nella tutela e nella protezione dei dati sensibili.

Aziende e cloud provider diventano, pertanto, i protagonisti del nuovo regolamento.

GDPR & DIGITALIZZAZIONE

brennercom
DATA PROTECTION
& SECURITY

Per rispondere alle attuali esigenze, Il **27 febbraio 2018** - al **NOI Techpark Südtirol** si è svolto l'evento "**GDPR Ready**" organizzato da **Brennercom** in collaborazione con **Effizient** e lo **studio Legale Guadagnini**. Un evento interamente dedicato al tema della sicurezza e della protezione dei dati. In questa occasione è stata fornita a tutti i partecipanti una visione dettagliata sia in termini legali, sia in termini infrastrutturali.

In questa logica, le imprese dovranno impegnarsi nell'aggiornare e implementare nuove attività per rispondere alle richieste dell'attuale normativa e i provider dei servizi cloud dovranno garantire la massima sicurezza delle loro piattaforme.

Brennercom - Cloud Provider – oltre ad essere conforme al nuovo regolamento, dispone di complesse e sicure reti private e internazionali e strumenti tecnologici adeguati, quali ad esempio sistemi di backup, next generation firewall (NGFW). Possiede, inoltre, una **piattaforma Cloud**, **certificata ISO 27001** ideale per assicurare la riservatezza e l'accessibilità dei dati oltre al digital workplace, un sistema di comunicazione integrata capace di offrire servizi di comunicazione all'avanguardia, utilizzabili da qualsiasi device.

I PRINCIPI NORMATIVI

brennercom
DATA PROTECTION
& SECURITY

Accountability - Principio di responsabilizzazione e rendicontazione.
Il Titolare del trattamento deve mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. Le misure da adottare vanno valutate di volta in volta, tenendo in considerazione una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Privacy by Design
I prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti. Il trattamento deve essere perciò previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati.

Privacy by Default
Per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

I CONTRATTI

L'imprenditore quale titolare del trattamento e figura che deve gestire i rapporti con gli outsourcer

LA GESTIONE DEI RAPPORTI CON I FORNITORI

brennercom
DATA PROTECTION & SECURITY

L'imprenditore, titolare del trattamento dei dati, dovrà gestire/trattare i dati ai sensi del GDPR. È pertanto necessario inserire una **clausola ad hoc** nei contratti che imponga al fornitore di:

- trattare i dati ai sensi del GDPR
- inserire analoga clausola nei contratti con eventuali subfornitori
- permetta all'imprenditore di effettuare periodici controlli (audit) presso il fornitore per verificare dette circostanze

LA GESTIONE DEI RAPPORTI CON I PARTNER

brennercom
DATA PROTECTION & SECURITY

L'imprenditore, titolare del trattamento dei dati, **e il partner sono contitolari del trattamento dei dati.**

Per questo motivo occorre:

- sancire la contitolarità del trattamento dei dati
- definire l'estensione della responsabilità di ciascuno
- descrivere i rapporti dei contitolari con gli interessati
- stabilire la possibilità di controlli reciproci (audit)

DATA PROTECTION OFFICER - DPO

La figura del DPO è una delle principali novità introdotte dal GDPR

DATA PROTECTION OFFICER - DPO

brennercom
DATA PROTECTION & SECURITY

Il **Data Protection Officer** è il responsabile della protezione dei dati; può essere dipendente del titolare del trattamento o un consulente esterno e ha una **conoscenza specialistica della normativa** e della prassi e che supporta il titolare nell'adempimento.

La figura del **DPO** risulta **obbligatoria** nei seguenti casi:

- Il trattamento dei dati è effettuato da un'autorità di un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali
- le attività principali del titolare del trattamento o del responsabile 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
- 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 o di dati relativi a condanne penali e a reati di cui all'articolo 10 (GDPR)

DATA PROTECTION OFFICER - DPO

brennercom
DATA PROTECTION & SECURITY

Compiti del DPO:

- Informare e fornire consulenza al Titolare, e ai suoi dipendenti; sorvegliare l'osservanza del Regolamento e delle altre normative in materia di dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo
- fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento
- cooperare con l'autorità di controllo
- fungere da punto di contatto per l'autorità di controllo.

brennercom

DATA PROTECTION
& SECURITY

8 PILLOLE FORMATIVE

PILLOLE FORMATIVE

brennercom
DATA PROTECTION & SECURITY

PILLOLA 1: MISURE DI SICUREZZA

Il Titolare del trattamento deve prevedere di base misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Esse sono:
l'autenticazione informatica
l'adozione di procedure di gestione delle credenziali di autenticazione
la protezione degli strumenti elettronici per evitare accessi non consentiti e la violazione dei dati (antivirus, firewall etc.)
l'adozione di procedure per la custodia di copie di sicurezza (backup)
codici identificativi per il trattamento di alcuni dati

PILLOLA 2: ACCESSO PROTETTO

Il Titolare del trattamento deve predisporre dei sistemi che consentano l'accesso ai dati unicamente al personale autorizzato. Dovrà quindi prevedere delle credenziali di autenticazione (a titolo esemplificativo nome utente e password, oppure accesso biometrico o accesso con una smart card) per accedere ai sistemi.
Ogni utente potrà accedere unicamente alle informazioni necessarie per svolgere le mansioni affidate.
Periodicamente, e comunque con cadenza annuale, occorre verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

PILLOLE FORMATIVE

brennercom
DATA PROTECTION & SECURITY

PILLOLA 3: SICUREZZA INFORMATICA

I dati personali devono essere protetti dal rischio di intrusione esterna e dall'azione di programmi in grado di violare la privacy.
Per questi motivi, dovranno essere predisposti idonei strumenti elettronici che siano in grado di prevenire la vulnerabilità dei sistemi e correggere eventuali difetti, quali ad esempio antivirus, antispyware e firewall, da tenere costantemente aggiornati.

PILLOLA 4: GESTIONE PASSWORD

Gli accessi alla postazione informatica e ai gestionali aziendali devono essere protetti da un sistema di autenticazione valido come ad esempio nome utente + password, oppure attraverso l'utilizzo di sistema biometrico o ancora inserendo nome utente + PIN etc.
La password deve essere composta da almeno 8 caratteri alfanumerici e dev'essere modificata periodicamente: almeno ogni 3 mesi se si trattano dati particolari (ex dati sensibili: stato di salute, vita sessuale, opinioni politiche, religiose, appartenenza al sindacato etc.) e/o dati relativi a condanne penali o reati (ex dati giudiziari).

PILLOLE FORMATIVE

brennercom
DATA PROTECTION & SECURITY

PILLOLA 5: STRUMENTAZIONE DIPENDENTI

All'interno delle organizzazioni occorre predisporre un regolamento interno che disciplini l'utilizzo degli automezzi aziendali e/o delle risorse telefoniche e informatiche assegnate ai dipendenti (es. smartphone, tablet, notebook etc).
Le risorse aziendali devono essere registrate e assegnate ai dipendenti con regolare lettera di assegnazione e assunzione di responsabilità.
Inoltre, è necessario individuare una figura responsabile della gestione e manutenzione delle risorse aziendali, nonché della gestione delle eventuali situazioni di emergenza (es. incidenti automobilistici, furto o smarrimento dello smartphone etc.).

PILLOLA 6: SISTEMI DI VIDEOSORVEGLIANZA

Nella struttura in cui è installata la VDS e sono presenti dipendenti - che possono essere ripresi, anche accidentalmente, durante l'orario di lavoro – occorre aver predisposto un accordo sindacale o ottenuto l'autorizzazione dell'ispettorato del lavoro per regolamentare l'installazione e l'utilizzo della VDS. Il tempo di conservazione delle immagini è di 24 ore salvo diversa esplicita autorizzazione dell'Ispettorato del lavoro o delle rappresentanze sindacali, massimo 7 giorni con loro consenso.
Le persone che accedono alle immagini dell'impianto VDS devono essere adeguatamente formate e informate sulle modalità di accesso e consultazione dei dati.

PILLOLE FORMATIVE

brennercom
DATA PROTECTION & SECURITY

PILLOLA 7: GEOLOCALIZZAZIONE

Per gli automezzi su cui è installato il GPS occorre predisporre un accordo sindacale o ottenere l'autorizzazione dell'ispettorato del lavoro per l'installazione e l'utilizzo dell'impianto GPS. Inoltre, è necessario aver effettuato la notifica obbligatoria al Garante della Privacy per il trattamento dei dati relativo al suo utilizzo.
Le persone che accedono ai dati di geolocalizzazione devono essere adeguatamente formate e informate sulle modalità di accesso e consultazione dei dati.

PILLOLA 8: ATTIVITA' DI MARKETING

Per tutte le attività di marketing rivolte all'esterno (newsletter, campagne di telemarketing, etc.) è necessario richiedere ai destinatari il consenso al trattamento dei dati. La medesima richiesta deve essere prevista anche per l'acquisto di banche dati (es: recapiti telefonici, indirizzi e-mail).
NOTA: Molto spesso la richiesta del consenso per finalità di marketing è a carico dell'acquirente della banca dati e non del venditore, se non la chiedi stai già trattando i dati in modo illecito!

L'IMPORTANZA DELLA CYBER SECURITY

brennercom
DATA PROTECTION & SECURITY

La violazione della sicurezza o data breach

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

Il titolare del trattamento che subisca un data breach deve darne **comunicazione tempestiva** e **comunque entro le 72 ore** all'autorità competente, a meno che sia improbabile che vi sia un rischio per i diritti e le libertà dell'interessato. In tale caso non dovrà essere fatta la notifica, ma deve essere tracciato in un registro interno.

GDPR ASSESSMENT

brennercom
DATA PROTECTION
& SECURITY

Una delle novità del GDPR è la valutazione d'impatto sulla protezione dei dati. Si tratta di una misura preventiva inerente il **Risk Assessment** che ciascun titolare del trattamento è tenuto ad effettuare sulla base della natura, dell'oggetto, del contesto e delle finalità del trattamento.

Brennercom in collaborazione con Effizient e lo studio Legale Guadagnini ha predisposto un **GDPR Assessment** per supportare i propri clienti nell' individuazione dei rischi derivanti dal trattamento e, quindi, dei mezzi e degli strumenti da adottare per contrastarli.

La finalità prevista dagli Assessment è di delineare lo stato dell'arte e definire i passi da intraprendere per essere conformi con la vigente normativa, **senza incorrere in sanzioni amministrative o, addirittura, penali.**

GDPR READY?
FAI SUBITO IL TEST GRATUITO

CONCETTI CHIAVE

brennercom
DATA PROTECTION & SECURITY

Dato personale: qualsiasi informazione riguardante una persona fisica che la renda identificabile.

Interessato: persona fisica identificata o identificabile. 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, i 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.

Titolare del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che determina le finalità ed i mezzi del trattamento di dati personali.

Responsabile del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Misure di sicurezza: Misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Registro delle attività di trattamento: documento gestito dal Titolare del trattamento o dal Responsabile del trattamento.
Tale deve contenere:

- nome e dati di contatto del titolare del trattamento, del contitolare, del rappresentante del titolare e del DPO;
- finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione dei dati;
- una descrizione generale delle misure di sicurezza tecniche ed organizzative.

PIA – Privacy Impact Assessment: Valutazione d'impatto sulla protezione dei dati, da effettuare quando un tratta mento può comportare un rischio elevato per i diritti degli interessati (per es. a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono trattati dati particolari etc.). Dev'essere fatta prima di iniziare il trattamento pericoloso, eventualmente consultando il Garante privacy se le misure di sicurezza individuate per ridurre il rischio non sembrano sufficienti.

REFERENCES

brennercom
DATA PROTECTION
& SECURITY

brennercom

In collaborazione con

STUDIO LEGALE Guadagnini

effizient® COMPANY SOLUTIONS

CONTACTS

brennercom

DATA PROTECTION
& SECURITY

brennercom

Via Pacinotti, 12
I-39100 Bolzano
Tel.+39 0471060111
Fax+39 0471060188
info@brennercom.it
www.brennercom.it