GDPR - Regolamento UE 2016/679

07 mar 2019

Indice

Suggerimento:

- - **Garante Privacy**. Panorama delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti per la piena applicazione del regolamento, prevista il 25/05/2018.
- sito **Garante Privacy**.
- **Quaderni ANCI** (febbraio 2018).
- .
- ()

Importante: Articolo di Altalex del 12 aprile 2018: . Tabella a cura di

Con questa tabella si offre a disposizione dell'utenza uno schema sintetico degli obblighi/adempimenti/cautele di spettanza del titolare del trattamento in base alle norme del (relativo alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali*).

Per una esigenza di articolazione e maggiore significatività della tabella, gli obblighi / adempimenti / cautele sono classificati come di seguito:

A fianco di ciascun argomento/voce la tabella riporta il riferimento (capo, articolo/i) nel testo del Regolamento.

REGOLAMENTO UE 2016/679: TABELLA RAGIONATA degli OBBLIGHI / ADEMPIMENTI / CAUTELE DEL TITOLARE

CAPITOLO 1

I principi applicabili al trattamento dei dati personali

CAPITOLO 2

Acquisizione del consenso da parte dell’interessato e casistica di esonero dal relativo obbligo

CAPITOLO 3

Il consenso dei minori a fronte di servizi ICT

CAPITOLO 4

Trattamento di particolari categorie di dati

CAPITOLO 5

Trattamento di dati relativi a condanne penali e reati

CAPITOLO 6

Trasparenza nella gestione dei trattamenti

CAPITOLO 7

Informativa all’interessato

CAPITOLO 8

Il rispetto dei diritti dell'interessato

CAPITOLO 9

Il particolare caso dei processi decisionali automatizzati

CAPITOLO 10

Misure di sicurezza adeguate

CAPITOLO 11

Privacy by design (fin dalla progettazione)

CAPITOLO 12

Privacy by default (per impostazione predefinita)

CAPITOLO 13

Contitolarità del trattamento

CAPITOLO 14

Nomina del Rappresentante del titolare

CAPITOLO 15

Nomina del Responsabile del trattamento

CAPITOLO 16

Obbligo di istruzione da parte del Titolare

CAPITOLO 17

Adozione del Registro delle attività di trattamento

CAPITOLO 18

Obbligo di cooperazione con l’autorità di controllo

CAPITOLO 19

Notificazione di una violazione dei dati

CAPITOLO 20

Comunicazione di una violazione dei dati all'interessato

CAPITOLO 21

Redazione della Valutazione d'impatto sulla protezione dati e consultazione dell'autorità di controllo

CAPITOLO 22

Nomina di un Responsabile della Protezione dei Dati (Data Protection Officer - DPO)

CAPITOLO 23

Adesione a codici di condotta/sistemi di certificazione

CAPITOLO 24

Cautele per il trasferimento dei dati in Paesi terzi

CAPITOLO 25

Obbligo di risarcimento del danno

CAPITOLO 26

MODULISTICA aggiornata al GDPR (scaricabile gratuitamente) a cura di Omnia Vis

in formato aperto

CAPITOLO 27

GDPR: 3 regole fondamentali per la conformità di un sito web

Importante: Fonte: di . 16 Aprile 2018

Esistono tre regole chiave da rispettare per rendere il proprio sito web conforme alle norme previste dal GDPR ovvero:

1. **Il consenso dell'utente.**
2. **L'accesso ai dati personali dell'utente.**
3. **La criptazione dei dati.**

27.1 Il consenso dell'utente

Il **consenso** è uno dei pilastri della nuova legislazione ed è vitale per poter salvare ed utilizzare i dati personali degli utenti. Dunque è necessario ottenere uno specifico permesso da parte dell'utente per poter trattare i suoi dati, **per qualsiasi motivo**.

I visitatori del sito web dovranno essere informati in modo preciso di come i loro dati verranno raccolti e trattati, sarà inoltre necessario informarli delle motivazioni di questa raccolta dati e sarà quindi molto importante che accettino di loro spontanea volontà selezionando un apposito form di conferma.

Prendiamo ad esempio le agenzia di collocamento, se un candidato approva il trattamento dei suoi dati personali ed invia il suo curriculum online per una determinata posizione, a meno che il campo di conferma da lui spuntato non reciti altro, l'agenzia non potrà sfruttare quel curriculum per proporre altre candidature né potrà cederlo ad altre aziende eventualmente interessante.

Dunque è bene che un sito web sia sempre aggiornato dal punto di vista delle informative e riceva dall'utente permessi espliciti ogni volta che dovessero essere previste nuove tipologie di trattamento dei dati personali.

Altra novità arrivata con la GDPR riguarda il linguaggio delle note sulla privacy dell'utente. Esse devono essere semplici da leggere e da comprendere per l'utente, dunque devono adottare un linguaggio comune e di facile interpretazione. Lo stesso dicasi per le comunicazioni sull'utilizzo dei cookie.

27.2 L'accesso ai dati

Il secondo componente chiave del GDPR è **l'accesso ai dati**. Bisogna rendere noto e avvertire l'utente su chi può accedere ai propri dati personali e come essi vengono registrati e conservati dal sito web, anche tramite CMS o CRM.

La via più semplice per farlo è in classico form dove si chiede all'utente di poter trattare, nei modi che si necessitano, i vari tipi di dati personali.

Se la risposta è negativa deve essere anche implementata una procedura per evitare che i dati vengano registrati e conservati, inoltre **deve essere sempre consentito all'utente di revocare tali permessi** in futuro e di cancellare i propri dati quando lo desidera. I titolari delle aziende dovrebbero inoltre verificare e controllare che le eventuali agenzie di terze parti che hanno accesso ai dati degli utenti abbiamo procedure conformi ai nuovi regolamenti.

27.3 La crittografia

Terze elemento cardine del GDPR è **la crittografia**. **Ogni dato dell'utente inviato e conservato su di un sito web dovrà essere criptato**, questo per impedire sottrazioni di informazioni sensibili tramite attacchi informatici.

Dunque ogni progetto che voglia essere conforme alla GDPR dovrà implementare un sistema che preveda l'utilizzo di certificati di sicurezza **SSL/TLS** durante le comunicazioni dei dati sensibili. Inoltre ai i vari database interni dovranno essere protetti da chiavi crittografiche «robuste» (qualsiasi sia il significato che si voglia attribuire a questo termine).

CAPITOLO 28

Altri articoli sull'applicazione del GDPR

28.1 Come adeguare la PA al GDPR: tutto ciò che bisogna fare

Importante: di Ernesto Belisario - agendadigitale.eu

nominare un (in italiano, RPD o responsabile della protezione dei dati personali).

Si tratta di una figura che deve possedere dei requisiti specifici (ad esempio in termini di esperienza e competenza, così come chiarito nelle) e deve occuparsi prevalentemente di informare e fornire consulenza sulla corretta applicazione della normativa, curando con particolare attenzione della formazione del personale.

È importante quindi notare che – così come previsto dalle Linee guida del gruppo Art. 29 – i DPO non rispondono personalmente in caso di inosservanza del GDPR.

Nomina del DPO. . . .il Data Protection Officer può essere interno o esterno. Nel primo caso, anche per salvaguardare la sua autonomia, non potrà coincidere con chi – all'interno dell'ente – definisce, anche in parte, le politiche di protezione dei dati personali (come il responsabile per la transizione digitale).

Trasparenza del trattamento. che si sostanzia nell'obbligo per il titolare di rendere l'informativa, cioè di dare evidenza – senza alcuna specifica richiesta – delle principali informazioni che riguardano il trattamento.

Registro dei trattamenti e misure di sicurezza. adozione entro il 25 maggio 2018 (e dell'aggiornamento continuo) di un registro delle attività di trattamento in cui descrivere:

1. il nome e i dati di contatto del titolare del trattamento e del DPO;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
5. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
6. una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione;

28.2 GDPR, tutto ciò che c'è da sapere per essere in regola

Importante: di Raffaella Natale - agendadigitale.eu

introdotta la **responsabilizzazione dei titolari del trattamento** (accountability) e un approccio che tenga in maggior considerazione i rischi che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Data Breach. Il titolare del trattamento dei dati personali al Garante. ed integrato e una maggiore cooperazione a livello Ue.

28.3 GDPR e diritto all'oblio

Importante: di Franco Pizzetti - agendadigitale.eu

La vera novità del diritto all'oblio. La parte veramente nuova, che consente di parlare anche di diritto l'oblio, pur poco avendo a che fare con l'informazione e la libertà di pensiero, riguarda il dovere specifico posto a carico del titolare che riceva una richiesta di cancellazione quando i dati che ne sono oggetto siano stati "resi pubblici" dal titolare stesso.

In questa ipotesi l'art. 17 paragrafo 2 impone al titolare non solo di cancellare i dati (sempre ovviamente che ritenga la richiesta legittima per quanto lo riguarda).

28.4 Formazione privacy obbligatoria, col Gdpr: che c'è da sapere

Importante: di Mauro Alovisio avvocato, docente corso di formazione del data protection officer - Università degli Studi di Torino, Costanza Mottino avvocato, esperto data protection. agendadigitale.eu

La **formazione costituisce**, pertanto, **un prerequisito** per potere operare all'interno delle organizzazioni, imprese e pubbliche amministrazioni.

La formazione dovrebbe essere finalizzata ad **illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni**.

Gli Enti pubblici le imprese, pertanto, **devono**:

– pianificare quanto prima un percorso ed un piano di formazione;

– accantonare adeguate risorse in sede di approvazione di bilancio, al fine di arrivare preparati alla scadenza del 25 maggio 2018, data in cui il Regolamento, già in vigore, esplicherà i suoi effetti;

– prevedere prove finali nel percorso formativo, e sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;

– individuare un percorso formativo alternativo, in caso di mancato superamento del test finale, ed un nuovo esame di verifica;

(*Le prove finali consentono di dimostrare il grado di conoscenza della normativa, delle istruzioni privacy all'interno dell'organizzazione*.)

Nelle previsioni di budget è necessario considerare anche risorse specifiche per la formazione del Data protection Officer e dei componenti del team.