Comuni di Boffalora Sopra Ticino, Marcallo con Casone, Ossona, Mesero

Incontro Gruppo PO privacy

19 04 2018

INDIVIDUAZIONE DEI SOGGETTI A CUI SI APPLICA IL REGOLAMENTO

Il Regolamento Europeo 679/2016 entra in vigore il 25 maggio 2018: disciplina il trattamento dei dati personali nonché le norme relative alla libera circolazione di tali dati. Il legislatore e l'autorità garante provvederanno ad armonizzare la normativa italiana (Dl.gvo 196/2003) alla norma europea.

DOVERE DI DOCUMENTARE ED INFORMARE

Una delle novità sostanziali introdotte dal regolamento è il principio dell'accountability (responsabilità verificabile), secondo cui tutti i soggetti che partecipano al trattamento dati devono essere consci e responsabili e devono tenere documentazione di tutti i trattamenti effettuati. le priorità fondamentali sono:

1. La designazione in tempi stretti del Responsabile della protezione dei dati (DPO);

2. L'istituzione del Registro delle attività di trattamento;

3. La notifica de(gli eventual)i *data breach* (e la introduzione di specifiche procedure da attivare a seguito delle eventuali violazioni).

Oltre alle priorità individuate dal Garante, appare importante attivarsi, prima del 25 maggio, per:

A. Aggiornare l'informativa, sulla base degli artt. 12 e ss del GDPR (tutte le P.O.);

B. Riesaminare le politiche interne in tema di trattamento di dati personali, ai sensi dell'art. 24 del GDPR, provvedendo anche a definire in maniera adeguata i ruoli e assicurarsi che tutti coloro che trattano dati personali ricevano adeguate istruzioni e formazione (ex art. 29 del GDPR) (Organi di vertice);

C. Procedere alla verifica dei sistemi informatici, per assicurare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all'art. 25 GDPR (concetti di privacy-by-default e privacy-by-design) (tutte le P.O.);

D. Esaminare i rapporti contrattuali con i responsabili esterni del trattamento, per verificarne la conformità (art. 28 del GDPR) (tutte le P.O.);

E. Verificare l'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR (D.P.O.);

F. Valutare se si debba procedere, per uno o più trattamenti, ad effettuare una valutazione d'impatto privacy (art. 35 del GDPR) (D.P.O.).

L’INFORMATIVA PRIVACY

L’informativa deve essere leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi.

Il primo

Deve essere fornita per iscritto (oralmente va bene SOLO se l’interessato è d’accordo e la sua identità deve comunque essere comprovata con altri mezzi).

Ciascuna posizione organizzativa dovrà provvedere ad effettuare una ricognizione della modulistica in uso ed adeguarla alla vigente normativa.

Il Gruppo P.O. Privacy nelle persone di Novarese e Bognetti provvederà ad inviare il format dell’informativa da inserire.

CAMBIA IL CONSENSO

Il consenso deve essere libero, specifico, informato e inequivocabile.

Il consenso è valido se la volontà è espressa in modo NON equivoco, anche con un'azione positiva: non ci deve essere per forza la casella di spunta, basta un testo in cui si informa che si accetta il trattamento dati con link all'informativa.
Gli uffici dovranno provvedere ad esporre una informativa completa all'interno dei locali.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Con il supporto del D.P.O. il titolare del trattamento, svolge una valutazione degli impatti privacy analizzando i rischi, definendo i gap rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando periodicamente gli effetti degli interventi per ridurre i rischi.

ABOLIZIONE DELLA NOTIFICAZIONE

Non si dovrà più notificare il Garante ogni violazione dei dati, ma ogni anno l'organizzazione dovrà redigere il Privacy Impact Assessment (P.I.A.), con il quale si considera effettuata la notifica.

IL DATA PROTECTION OFFICER (DPO)

Gli enti pubblici dovranno individuare un responsabile per la protezione dei dati (soggetto diverso dal responsabile del trattamento di cui all'art. 4 del Regolamento Eu).

Il DPO (di cui agli artt. 37/39), garante della sicurezza del trattamento dei dati, sarà una figura manageriale con rinnovo periodico, sarà referente del Garante e dovrà avere requisiti e competenze elevate.

Il DPO, negli enti della nostra dimensione, dovrà necessariamente essere un collaboratore esterno di comprovata professionalità ed ingaggiato con regolare contratto e incarico.

Avrà anche il compito specifico di vigilare e garantire che i processi lavorativi trattino i dati conformemente alla normativa vigente.

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

La privacy deve essere vista come un elemento strutturale del procedimento:

E’ essenziale avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro.

La ricognizione sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso

OBBLIGO DI SEGNALAZIONE IN CASO DI VIOLAZIONE DEI DATI (Data Breach)

Nel caso di violazione del trattamento dati bisogna effettuare una segnalazione al Garante entro 72 ore dall'evento e, nel più breve tempo possibile, bisogna informare anche i diretti interessati.

Occorre valutare la probabilità che gli individui abbiano conseguenze avverse sui loro diritti fondamentali, a seguito del fatto certo di uno specifico data breach

- **Tipo di data breach (vulnerabilità del sistema informatico, password deboli, dipendente infedele …)**
- **Natura e quantità dei dati personali**
- **Facilità di identificazione degli individui**
- **Gravità delle eventuali conseguenze per gli individui**
- **Individui "speciali" (ad es: bambini)**
- **Numero degli individui coinvolti**
- **Caratteristiche "speciali" del Titolare (ad es: ospedale)**

RICONOSCIMENTO DI NUOVI DIRITTI

Il Regolamento EU individua accanto a quelli già esistenti, nuovi diritti degli interessati:

diritto di accesso (ricevere copia dei dati personali oggetto del trattamento),

diritto alla cancellazione (diritto all'oblio),

diritto di limitazione del trattamento,

diritto alla portabilità dei dati (posso pretendere che il soggetto a cui ho concesso l'uso dei miei dati me li restituisca su un supporto elettronico strutturato così che io possa farne ulteriore uso, anche presso un altro fornitore),

IPOTESI ORGANIGRAMMA E PROCEDURE

Brainstorming

SOGGETTI E RUOLI

Titolare del trattamento: il Comune

Responsabile del trattamento: esistono responsabili interni (le P.O.) e responsabili esterni (persone giuridiche che trattano dati per conto del comune – rivedere i contratti in essere e le nomine e i proprietari dei Data Base)

Responsabile della sicurezza dei dati: DPO

ADEMPIMENTI

Avvio procedimento:

raccolta e studio DPS approvati negli anni precedenti;

analisi dei livelli di sicurezza delle piattaforma informatiche attualmente in uso

mappatura servizi a carico delle singole P.O,

schema registro trattamento

ricognizione modulistica attualmente in uso

verifica idoneità e revisione con riferimento Reg EU (ancorché non siano state ancora formulate indicazioni dall'autority e dal Legislatore *)*

Nomina D.P.O. (ENTRO IL 25 MAGGIO 2018) – Stesura del Protocollo di intesa tra enti, reperimento e stanziamento risorse a bilancio