COMUNICATO STAMPA

EDPS/2016/08

Bruxelles, 21 marzo 2016

Guida del GEPD alla messa in sicurezza delle informazioni e della continuità operativa

Nella sua **Guida** sulla *gestione dei rischi legati alla sicurezza delle informazioni* pubblicata in data odierna, il Garante europeo della protezione dei dati (GEPD) fornisce suggerimenti alle istituzioni dell'UE su come garantire un ambiente digitale sicuro e affidabile per le informazioni che sono essenziali per il funzionamento dei loro servizi.

Il GEPD aggiunto, Wojciech Wiewiórowski, ha affermato: *"La sicurezza dei dati personali è un obbligo di legge, ma è anche necessaria nell'interesse delle organizzazioni che si affidano all'uso di informazioni per la loro attività quotidiana. È essenziale che esse mantengano livelli di sicurezza adeguati per le informazioni in quanto il valore e l'efficienza del loro lavoro dipende in modo rilevante da ciò. Esorto le gerarchie delle istituzioni dell'UE a impegnarsi nello sviluppo e nell'uso di processi personalizzati di gestione dei rischi legati alla sicurezza delle informazioni in modo da rispondere alle esigenze specifiche della loro organizzazione".*

Organizzazioni diverse sono esposte a rischi diversi per la sicurezza relativi alle informazioni che utilizzano; pertanto, metodi evoluti di valutazione del rischio forniscono un modo efficace per individuare le soluzioni adeguate per i rischi specifici affrontati da una data istituzione e possono giustificare l'uso di risorse finanziarie e informatiche per sviluppare tali soluzioni.

La gestione dei rischi legati alla sicurezza delle informazioni relative a dati personali richiede competenze specialistiche in materia di sicurezza informatica e delle informazioni, nonché di protezione dei dati. I responsabili della protezione dei dati (RPD) dovrebbero sostenere gli esperti di sicurezza informatica e delle informazioni nello sviluppo di questi processi.

Le soluzioni tecniche di sicurezza da sole non possono risolvere il problema della sicurezza delle informazioni. La dirigenza di un'organizzazione ha, in ultima analisi, la responsabilità dell'attuazione delle decisioni che riguardano le applicazioni e le infrastrutture informatiche che sono di supporto all'organizzazione stessa. La dirigenza deve sostenere lo sviluppo e l'attuazione di politiche e mobilitare le risorse necessarie per contrastare i rischi relativi alle informazioni che un'organizzazione deve affrontare.

Sebbene la presente Guida sia essenzialmente rivolta alle istituzioni dell'UE, qualunque soggetto interessato alla protezione dei dati può trovarla utile; il regolamento sulla protezione dei dati applicabile alle istituzioni dell'UE (regolamento (CE) n. 45/2001) è simile per molti aspetti alla direttiva 95/46/CE relativa alla protezione dei dati, recepita nel diritto nazionale degli Stati membri dell'UE, nonché in Islanda, nel Liechtenstein e in Norvegia.

La presente Guida continuerà ad essere utile con l'entrata in vigore del nuovo regolamento generale sulla protezione dei dati che conserva il principio della gestione dei rischi per la sicurezza e rafforza le esigenze generali di responsabilità e di governance, introducendo esplicitamente il principio di **responsabilità** nel rispettare gli obblighi di protezione dei dati.

Informazioni di riferimento

Le disposizioni in materia di protezione dei dati nelle istituzioni dell'UE, nonché i doveri del Garante europeo della protezione dei dati (GEPD), sono definiti nel **regolamento (CE) n. 45/2001**. Il GEPD è un'autorità di vigilanza indipendente relativamente nuova ma sempre più influente, che controlla il trattamento dei dati personali da parte delle istituzioni e degli organismi dell'UE, fornisce pareri sulle politiche e sulle norme che interessano la sfera della privacy e coopera con autorità analoghe per garantire una protezione omogenea dei dati.

Giovanni Buttarelli (GEPD) e **Wojciech Wiewiórowski** (GEPD aggiunto) sono membri dell'istituzione, nominati con decisione congiunta del Parlamento europeo e del Consiglio, con mandato quinquennale. Sono entrati in carica il 4 dicembre 2014.

Informazioni o dati personali: qualsiasi informazione concernente una persona fisica (vivente) identificata o identificabile, ad esempio nome, data di nascita, fotografie, filmati, indirizzi e-mail e numeri di telefono. Anche altri dettagli come ad esempio gli indirizzi IP e il contenuto di comunicazioni – relativi a o forniti da utenti finali di servizi di comunicazioni – sono considerati dati personali.

Privacy: il diritto di essere lasciati in pace e di avere il controllo delle proprie informazioni personali. Il diritto alla privacy o vita privata è sancito dalla Dichiarazione universale dei diritti dell'uomo (articolo 12), dalla Convenzione europea dei diritti dell'uomo (articolo 8) e dalla Carta dei diritti fondamentali dell'Unione europea (articolo 7). La Carta prevede anche il diritto esplicito alla protezione dei dati di carattere personale (articolo 8)

Trattamento dei dati personali: ai sensi dell'articolo 2, lettera b), del regolamento (CE) n. 45/2001, per trattamento di dati personali s'intende «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, l'allineamento o l'interconnessione, nonché il blocco, la cancellazione o la distruzione». Si veda a questo proposito il glossario disponibile sul sito del GEPD.

L'**articolo 22 del regolamento 45/2001** contiene la prescrizione che impone alle istituzioni dell'UE di mitigare i rischi nell'ambito del trattamento dei dati personali.

- Nelle analisi, la gestione dei rischi legati alla sicurezza delle informazioni deve includere anche i rischi legati alla sicurezza delle informazioni che interessano dati personali;
- dall'analisi dei rischi può scaturire la definizione e l'attuazione di una serie di adeguate misure di sicurezza.

Le misure di sicurezza che proteggono i dati personali non possono essere definite in modo generico, in quanto devono derivare dal processo di gestione dei rischi legati alla sicurezza delle informazioni che tiene conto del contesto specifico nel quale sono trattati i dati personali.

Gli **esperti in sicurezza delle informazioni** sono specializzati nello sviluppare soluzioni per proteggere i sistemi informativi e le informazioni contro accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzati.

Gli **esperti di sicurezza informatica** sono specializzati nello sviluppare soluzioni per proteggere le informazioni che utilizzano varie forme di tecnologia per creare, memorizzare, usare e scambiare tali informazioni contrastando accessi non autorizzati, uso improprio, malfunzionamenti, modifiche, distruzioni o divulgazioni improprie.

Il Garante europeo della protezione dei dati (GEPD) è un'autorità di vigilanza indipendente incaricata di proteggere i dati personali e la privacy e di promuovere buone prassi nelle istituzioni e negli organismi dell'UE. Nello svolgimento dei suoi compiti, il Garante:

- vigila sul trattamento dei dati personali da parte dell'amministrazione dell'UE;
- formula pareri sulle politiche e sulla legislazione che interessano la privacy;
- coopera con autorità simili per garantire una protezione omogenea dei dati.

La Guidadel GEPD è disponibile sul sito web del GEPD.

Eventuali domande possono essere inviate a: press@edps.europa.eu

GEPD – Il guardiano europeo della protezione dei dati personali

www.edps.europa.eu

Seguiteci su Twitter: @EU_EDPS