PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4841 di Lunedì 21 dicembre 2020

Una guida per sviluppare il documento ex articolo 25 del GDPR

Il regolamento generale europeo impone che per tutti i trattamenti, sia informatizzati, sia cartacei, venga sviluppato un documento, che illustri le modalità di protezione dei dati incorporate del progetto iniziale e per impostazione predefinita.

Purtroppo, a molti titolari del trattamento è ancora sfuggito il fatto che il nuovo regolamento generale sulla protezione dei dati impone a tutti i titolari di sviluppare un documento, che illustri i criteri utilizzati per la protezione dei dati da trattare.

Questo obbligo è assolutamente generale e si applica sia a trattamenti informatici, sia a trattamenti cartacei. L'articolo 25 del regolamento europeo illustra in dettaglio i contenuti di questo documento.

Purtroppo, ancora oggi moltissimi trattamenti vengono effettuati dai titolari, senza che sia stata rispettata questa disposizione e ciò può portare all'applicazione, soprattutto in caso di perdite o violazione di dati, di gravi sanzioni per i soggetti coinvolti.

Ecco il motivo per cui il comitato europeo per la protezione dei dati si era già attivato nel 2019, mettendo a disposizione una bozza di linee guida per lo sviluppo del documento ex articolo 25, che oggi sono state ufficialmente pubblicate, dopo l'approvazione ricevuta da tutte le autorità Garanti nazionali.

Il fatto che queste linee guida siano state validate dal comitato europeo per la protezione dei dati permette altresì ai titolari del trattamento, che operino in varie nazioni europee, di sviluppare un unico documento che dovrà essere necessariamente accettato dalle autorità garanti nazionali dei vari paesi.

Queste linee guida danno delle indicazioni generali, che permettono ai titolari del trattamento di rispettare l'obbligo di elaborare il documento previsto dall'articolo 25.

È bene ricordare che lo sviluppo di questo documento è obbligatorio per qualunque tipo di trattamento e quindi rientra fra i primi obblighi che gli ispettori delle autorità garanti nazionali andranno a verificare, in caso di ispezione.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

L'obbligazione di base, nell'effettuare un trattamento di dati personali, impone l'attuazione di misure appropriate e di appropriate salvaguardie, che garantiscano il rispetto dei principi di protezione dei dati e quindi i diritti e le libertà degli interessati coinvolti.

Già abbiamo avuto occasione di fare presente che l'espressione inglese "protection by default" è stata in italiano tradotta con l'espressione "protezione per impostazioni predefinite".

Il documento ex articolo 25 deve essere sviluppato prima di iniziare il trattamento e deve essere continuamente tenuto aggiornato, per essere certi che le misure di protezione dei dati siano allineate con eventuali nuovi rischi, introducendo appropriate salvaguardie. Il fatto che, alla data di entrata in vigore del regolamento europeo, molti trattamenti fossero già in essere non esonera il titolare dall'obbligo di sviluppare subito questo documento, applicabile ai trattamenti in essere.

Le linee guida offrono preziose indicazioni su come attuare i principi di protezione dei dati, elencati nell'articolo 5 del regolamento, elencando le varie tipologie di dati trattati e le specifiche modalità di protezione. Il documento inoltre raccomanda che i titolari ed i responsabili del trattamento cooperino strettamente nello sviluppo di questo documento.

Se poi questo documento fa riferimento a certificazioni o codici di condotta, tanto di guadagnato.

Le linee guida successivamente si concentrano sulla interpretazione dei requisiti elencati nell'articolo 25, illustrando gli obblighi legali introdotti da questo articolo. Vengono anche offerte delle esemplificazioni specifiche nell'attuazione dei principi di protezione dei dati, che devono essere rispettati.

Ricordo ai lettori che i principali obblighi da rispettare, nell'effettuare una qualunque attività di trattamento di dati sono i seguenti:

- trasparenza,
- legittimità,
- correttezza,
- limitazione delle finalità,
- minimizzazione dei dati raccolti,
- accuratezza dei dati,
- limiti alla durata di conservazione dei dati,
- integrità e riservatezza,
- responsabilizzazione dei soggetti coinvolti.

Infine, il documento esamina la possibilità che possa essere attivato un meccanismo di certificazione applicabile al documento ex articolo 25. Ricordo che al momento non esistono schemi di certificazione applicabili, ma non v'è dubbio che un ente di certificazione riconosciuto, che si attivi su questo fronte, potrebbe incontrare un successo commerciale non indifferente.

Il documento si chiude con alcune indicazioni specialmente indirizzate alle piccole e medie industrie, per cercare di alleviare, per quanto possibile, l'impegno richiesto dall'elaborazione di questo documento, in un contesto aziendale che ha poco spazio per

sostenere ulteriori oneri procedurali.

In chiusura di questo appunto, mi permetto di ricordare a tutti i lettori che, se comprano dei software da parte di software house esterne, questo documento deve essere fornito insieme al software stesso. Un meglio, la software house deve fornire una traccia del documento, dove alcune aree evidentemente saranno completate dal titolare del trattamento, perché queste aree fanno riferimento a specifiche applicazioni.

Per fortuna, già oggi parecchie software house si sono attivate in questo senso e confido che presto tutte potranno mettere a disposizione dei clienti questo prezioso è necessario documento.

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (pdf)

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it