Consiglio dell'UE

PRESS
IT

COMUNICATO STAMPA
951/15
18.12.2015

Riforma della protezione dei dati nell'UE: il Consiglio conferma l'accordo con il Parlamento europeo

Il 18 dicembre 2015 il Comitato dei rappresentanti permanenti (Coreper) ha confermato i testi di compromesso concordati con il Parlamento europeo sulla riforma della protezione dei dati. L'accordo tra Consiglio, Parlamento e Commissione è stato raggiunto il 15 dicembre. Detto accordo è in linea con la richiesta di negoziati sulla riforma della protezione dei dati, da concludere entro la fine del 2015, formulata dal Consiglio europeo.

Félix BRAZ, ministro della giustizia lussemburghese e presidente del Consiglio, ha dichiarato: "È un accordo fondamentale che avrà conseguenze importanti. Questa riforma non solo rafforza i diritti dei cittadini, ma adegua anche le norme all'era digitale per le imprese, riducendo nel contempo gli oneri amministrativi. Si tratta di testi ambiziosi e lungimiranti. Possiamo avere piena fiducia nei risultati."

La riforma della protezione dei dati è un pacchetto legislativo proposto dalla Commissione nel 2012 per aggiornare e modernizzare le norme in materia. Riguarda due strumenti legislativi: il regolamento generale sulla protezione dei dati (inteso a sostituire la direttiva 95/46/CE) e la direttiva sulla protezione dei dati nel settore delle attività di contrasto (intesa a sostituire la decisione quadro sulla protezione dei dati del 2008).

La tutela delle persone rispetto al trattamento dei dati di carattere personale è un diritto fondamentale sancito dalla Carta dei diritti fondamentali dell'UE (articolo 8) e dal trattato sul funzionamento dell'Unione europea (articolo 16).

Regolamento generale sulla protezione dei dati

Il regolamento generale sulla protezione dei dati mira a rafforzare il livello di protezione dei dati per le persone fisiche i cui dati personali sono oggetto di trattamento e a migliorare le opportunità per le imprese nel mercato unico digitale anche attraverso la riduzione degli oneri amministrativi.

Un livello rafforzato di protezione dei dati

I principi e le norme in materia di trattamento dei dati personali delle persone fisiche devono rispettare i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali. Il rafforzamento dei diritti di protezione dei dati offre agli interessati (le persone fisiche i cui dati personali vengono trattati) un maggiore controllo sui loro dati personali:

- norme più specifiche che consentano ai responsabili del trattamento (incaricati di trattare i dati) di trattare i dati personali, anche attraverso l'obbligo del consenso delle persone fisiche interessate
- accesso facilitato ai propri dati personali
- una migliore informazione su quanto accade ai dati personali una volta condivisi. Ciò comporta l'informazione delle persone fisiche sulla politica di tutela della riservatezza con un linguaggio semplice e chiaro, anche utilizzando icone standardizzate
- un diritto alla cancellazione dei dati personali e "all'oblio", il che consente, ad esempio, agli interessati di chiedere la soppressione, senza ritardo, dei dati personali raccolti o pubblicati su una rete sociale quando la persona fisica era ancora un minore
- se un giovane di meno di 16 anni desidera utilizzare servizi in linea, il prestatore deve cercare di verificare l'effettivo consenso dei genitori. Gli Stati membri possono abbassare tale limite d'età senza scendere sotto i 13 anni
- un diritto alla portabilità, che facilita la trasmissione dei dati personali da un prestatore di servizi, quale una rete sociale, a un altro. Si avranno così non solo maggiori diritti in materia di protezione dei dati, ma anche una maggiore concorrenza tra prestatori di servizi
- un diritto a opporsi al trattamento dei dati personali inerenti all'interesse pubblico o ai legittimi interessi di un responsabile del trattamento. Tale diritto concerne l'uso dei dati personali a fini di "profilazione"
- garanzie comuni concernenti il trattamento dei dati personali a fini di archiviazione qualora ciò sia nell'interesse pubblico e per finalità di ricerca scientifica e storica o a fini statistici

Per garantire la prossimità dell'accesso alla giustizia, gli interessati hanno diritto a far riesaminare dalle autorità giurisdizionali nazionali una decisione dell'autorità per la protezione dei dati, a prescindere dallo Stato membro in cui è stabilito il responsabile del trattamento.

Migliori opportunità per le imprese nel mercato unico digitale

Il regolamento prevede un insieme unico di regole, valido in tutta l'UE e applicabile alle imprese sia europee che non europee che offrono servizi online nell'UE. Ciò consente di evitare una situazione in cui norme nazionali divergenti in materia di protezione dei dati possano ostacolare lo scambio di dati transfrontaliero. È inoltre prevista una maggiore cooperazione tra gli Stati membri per garantire l'applicazione coerente delle norme sulla protezione dei dati in tutta l'UE. Si creeranno così condizioni di concorrenza leali e le imprese, soprattutto le piccole e medie imprese, saranno incoraggiate a trarre il massimo beneficio dal mercato unico digitale.

Per ridurre i costi e offrire la certezza del diritto, nei casi transfrontalieri importanti in cui sono coinvolte diverse autorità di controllo nazionali, si adotterà una decisione di controllo unica. Questo **meccanismo di sportello unico** consente a un'impresa che opera in vari Stati membri di trattare solo con l'autorità per la protezione dei dati dello Stato membro in cui ha lo stabilimento principale. Il meccanismo prevede anche, in caso di controversie, una decisione unica applicabile in tutto il territorio dell'UE.

Al fine di ridurre i costi amministrativi, il regolamento applica un approccio basato sul rischio: i responsabili del trattamento possono attuare misure proporzionate al rischio insito nei trattamenti da essi effettuati. Imprese diverse svolgono attività diverse e i rischi di tali attività in termini di riservatezza possono variare. Il regolamento non prevede una soluzione unica in tutti i casi: quanto maggiori sono i rischi delle attività per i dati personali, tanto più rigorosi sono gli obblighi.

Maggiori strumenti di migliore qualità per far rispettare le norme in materia di protezione dei dati

Il regolamento prevede una serie di misure intese ad aumentare la responsabilità dei responsabili del trattamento, al fine di garantire il pieno rispetto delle nuove norme in materia di protezione dei dati. I responsabili del trattamento devono attuare una serie di misure di sicurezza, compreso l'obbligo, in taluni casi, di comunicare le violazioni dei dati personali. Per poter adeguare il regolamento alle esigenze future, sono stati introdotti i principi di protezione fin dalla progettazione e di protezione di default. Le autorità pubbliche e le imprese che svolgono talune operazioni rischiose di trattamento dei dati devono designare un **responsabile della protezione dei dati** incaricato di garantire il rispetto delle norme.

Gli interessati e, in determinate circostanze, le organizzazioni per la protezione dei dati possono presentare un reclamo all'autorità di controllo o proporre un ricorso giurisdizionale in caso di non rispetto delle norme in materia di protezione dei dati. I responsabili del trattamento possono incorrere in sanzioni che ammontano fino a 20 milioni di EUR o al 4 % del loro fatturato globale annuo.

Garanzie sul trasferimento di dati personali al di fuori dell'UE

Il regolamento stabilisce le norme per il trasferimento di dati personali verso paesi terzi e organizzazioni internazionali. I trasferimenti sono possibili a condizione che siano soddisfatte un certo numero di condizioni e garanzie, in particolare quando la Commissione ha deciso che esiste un livello di protezione adeguato. Le nuove decisioni di adeguatezza dovranno essere riesaminate almeno ogni 4 anni. Le decisioni e autorizzazioni di adeguatezza esistenti restano in vigore fino a quando non vengono modificate, sostituite o abrogate.

Direttiva sulla protezione dei dati nel settore delle attività di contrasto

La direttiva mira a proteggere i dati personali trattati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, inclusa la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

È fondamentale garantire un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche facilitando al tempo stesso lo scambio di dati personali tra i servizi di contrasto nei diversi Stati membri.

Campo di applicazione più ampio

Oltre a riguardare le attività volte a prevenire, indagare, accertare o perseguire reati, la nuova direttiva è stata ampliata in modo da comprendere la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

La nuova direttiva si applicherà sia al trattamento transfrontaliero dei dati personali, sia al trattamento dei dati personali da parte delle autorità giudiziarie e di polizia a livello puramente nazionale. La decisione quadro, che sarà sostituita, riguardava soltanto lo scambio transfrontaliero di dati.

Diritti degli interessati

Le norme raggiungono un equilibrio tra il diritto alla riservatezza e la necessità per la polizia di non rivelare i dati in corso di trattamento in una fase precoce delle indagini. Tuttavia, il testo contiene l'elenco delle informazioni che l'interessato è sempre autorizzato a ricevere per tutelare il suo diritto se teme che i propri dati siano stati violati.

Le nuove norme riguarderanno anche il trasferimento dei dati personali verso paesi terzi e organizzazioni internazionali.

Conformità

La nuova direttiva prevede che sia nominato un **responsabile della protezione dei dati** incaricato di aiutare le autorità

competenti a garantire la conformità alle norme in materia di protezione dei dati.

Un altro strumento per garantire la conformità è la valutazione d'impatto. Se è probabile che un tipo di trattamento comporti un rischio elevato per i diritti e le libertà delle persone fisiche, le autorità competenti devono effettuare una valutazione dell'impatto potenziale di un determinato trattamento, specie in caso di utilizzo di nuove tecnologie.

Controllo e risarcimento

Il testo della direttiva è allineato al testo del regolamento al fine di garantire che, in linea generale, valgano gli stessi principi generali. Inoltre, le norme sull'autorità di controllo sono in larga misura simili, in quanto l'autorità di controllo prevista dal regolamento generale sulla protezione dei dati può anche occuparsi delle questioni rientranti nella direttiva. La nuova direttiva concederà inoltre agli interessati il diritto al risarcimento per eventuali danni subiti a seguito di un trattamento non conforme alle norme previste.

FASI SUCCESSIVE

Il 17 dicembre, in una riunione straordinaria, la commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo (LIBE) ha approvato i testi concordati nei triloghi. Tale sostegno ha consentito oggi al Coreper di confermare i testi di compromesso finali relativi al regolamento e alla direttiva. Una volta messi a punto dai giuristi-linguisti, saranno sottoposti all'adozione da parte del Consiglio e, successivamente, del Parlamento. Il regolamento e la direttiva entreranno probabilmente in vigore nella primavera del 2018.

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press