Sistemi IT della P.A e Privacy by design

Autore: Redazione
In:

La Pubblica Amministrazione, al pari di ogni altro titolare di un trattamento di dati personali, è tenuta ad adottare idonee misure logiche di sicurezza a protezione dei propri sistemi informatici.
Pertanto, anche le banche dati della Pubblica Amministrazione sono state oggetto di provvedimenti da parte dell'Autorità Garante, finalizzati ad aumentare lo standard delle misure di sicurezza.
Tra questi, è il caso di ricordare il Provvedimento 2 luglio 2015 «Misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni pubbliche» (G.U. n. 179, serie generale, del 4 agosto 2015) [doc. web n. 4129029], con il quale il Garante ha dettato tutta una serie di misure di sicurezza alle quali le P.A. devono attenersi. Vista l'attinenza con l'istituto della data brech notification del nuovo regolamento europeo 679/2016[1], merita ricordare che il Garante ha prescritto che le Amministrazioni dello Stato – compresi gli istituti e le scuole di ogni ordine e grado, le Regioni e le Province, anche quelle autonome, i Comuni, le aziende e gli enti del Servizio sanitario nazionale e gli enti pubblici non economici – debbano comunicare allo stesso Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni o gli incidenti informatici (i c.d. 'data breach') che possono avere un impatto significativo sui dati personali contenuti nelle banche dati. Le comunicazioni devono essere redatte secondo il modello messo a disposizione dalla stessa Autorità Garante ed inviato via mail all'indirizzo «databreach.pa@pec.gpdp.it».[2]
[1] Si tratta di un istituto tra i più innovativi introdotto dagli articoli 33 e 34 del RGPD 679/2016. Esso consiste nell'effettuare una notificazione all'Autorità Garante da parte del Titolare del trattamento non appena viene a conoscenza di una violazione dei dati personali. La notificazione va effettuata, senza ingiustificato ritardo e, se possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Non si tratta di una novità assoluta in quanto l'istituto è stato introdotto dalla Direttiva 2009/136/CE, che, modificando l'articolo 4 della Direttiva 2002/58/CE ha previsto che in caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente. Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata. La novità sta ora nel fatto che il Regolamento amplia l'istituto ad ogni tipo di trattamento.
[2] Per maggiori approfondimenti si rinvia a 'Privacy – Protezione e trattamento dei dati' a cura di M. Soffientini, IPSOA 2016, pag.569.
Alla luce del nuovo regolamento Ue 679/2016, che troverà piena applicazione a partire dal 25 maggio 2018, anche la Pubblica Amministrazione dovrà perseguire l'obiettivo di implementare un Sistema di Gestione Privacy capace di proteggere i dati, riducendone al minimo l'utilizzazione. Sotto questo profilo, il regolamento introduce i principi della data protection by design and by default.
Con l'espressione data protection by design[1], disciplinata dal paragrafo 1 dell'articolo 25[2] del RGPD

Diritto & Diritti ISSN 1127-8579

679/2016, si intende l'obbligo in capo al Titolare, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura e delle finalità del trattamento, di mettere in atto misure tecniche e organizzative adeguate, per integrare nel trattamento le necessarie garanzie volte a tutelare i diritti degli interessati.
In altri termini, la data protection by design significa il rispetto dei principi di data protection attraverso la loro protezione fin dalla fase di progettazione di un trattamento di dati personali. [3]
Secondo lo spirito della norma, il Titolare dovrà adottare misure tecniche e organizzative che spingano verso una maggiore riservatezza del dato oppure trattare i dati in modo da minimizzarne l'uso. Ad esempio, la norma richiama la tecnica di pseudonimizzazione[4] come idonea ad attuare in modo efficace i principi di protezione dei dati sotto il profilo della minimizzazione.
L'applicazione di tecniche idonee a rispettare i principi della data protection introduce il concetto della data protection by default, che è definito dal paragrafo 2 dell'articolo 25 del RGPD 679/2016[5]. Si tratta di un concetto molto importante quando si ha a che fare con trattamenti automatizzati, perché sta a significare che la protezione di un trattamento di dati personali è garantita da impostazioni predefinite (di 'default').
La finalità della data protection by design è quella di rendere i trattamenti compliant alla disciplina sulla protezione dei dati personali, mentre la finalità della data protection by default attiene alla protezione del trattamento automatizzato da accessi non consentiti e per finalità diverse, attraverso la configurazione di impostazioni che di 'default' consentono il rispetto della disciplina sulla protezione dei dati personali.
Entrambi questi concetti sono destinati a giocare un ruolo fondamentale in termini di responsabilità giuridica anche per la P.A., in quanto nel Regolamento (art. 24) il Titolare (controller) è tenuto ad assumere tutte le misure, tecniche e organizzative, necessarie per consentire di 'dimostrare' che i trattamenti da lui posti in essere sono conformi alla normativa.[6]
[1] Il concetto di privacy by design è stato sviluppato per primo dal Commissario dell'Autorità Garante canadese della provincia dell'Ontario, Ann Cavoukian nel 2009. Vedi 'Privacy by design, the 7 fundamental principles' consultabile al seguente link: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
[2] Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. (Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights

Diritto & Diritti ISSN 1127-8579

of data subjects).
[3] Vedi Privacy e Regolamento Europeo di A. Ciccia Messina N. Bernardi, IPSOA 2016, pag. 41.
[4] I processi di pseudonimizzazione consistono nellapplicazione di un insieme di tecniche che consistono nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile. In questo modo si rende più complessa lidentificazione della persona. Per maggiori approfondimenti si veda: Big Data e Privacy by design di G. DAcquisto e M. Naldi, Giappichelli 2017, pag. 37.
[5] Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. (The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.).
[6] Si veda Privacy e il diritto europeo alla protezione dei dati personali di F. Pizzetti, Giappichelli 2016, pag. 283.
Leggi lo speciale: Riforma pubblica amministrazione

https://www.diritto.it/sistemi-it-della-p-a-e-privacy-by-design/

Diritto & Diritti ISSN 1127-8579