Versione italiana
English version

Feedback sulle "Linee guida 4/2019 sull'articolo 25 Protezione dei dati in base alla progettazione e per impostazione predefinita"
Feedback on '4/2019 Guidelines on Article 25 Data Protection by Design and by Default'

***

"Non si tratta di fornire all'individuo un *habeas scriptum*, come mezzo di difesa contro l'elaboratore, ma di consegnargli quest'ultimo come mezzo di controllo e partecipazione sociale"
Stefano Rodotà "Elaboratori elettronici e controllo sociale" (Bologna 1973, Il Mulino)

"It is not about providing people an *habeas scriptum*, as a way of defense against the computer, but giving people the computer, as a way of control and social participation"
Stefano Rodotà "Elaboratori elettronici e controllo sociale" (Bologna 1973, Il Mulino)

.

Paragrafo 2 - Analisi dell'articolo 25
1a Il Data Manager (Principle 1. Proactive not Reactive; Preventative not Remedial[1])
Operare secondo privacy by design e by default implica competenze sempre più complesse specie in relazione all'evoluzione delle tecnologie dell'informazione e della comunicazione.
Considerando che la gestione dei dati in generale costituisce una attività a crescente valore aggiunto in relazione alla capacità di trarne informazioni utili sia agli operatori di mercato per sfruttarle a fini di business sia agli operatori pubblici per migliorare gli aspetti di governance e gli outcome della loro attività, si ritiene che una best practice da promuovere a cura dei Titolari sia quella di formalizzare una strategia di Data managenent.
Specie nelle realtà più complesse, (la Funzione di) il Data Manager sarebbe l'attore che per conto dell'Organo di vertice (e del Titolare ex-GDPR) definisce l'architettura di gestione del patrimonio dati in una ottica olistica, in grado di promuovere una policy da applicare con coerenza in ogni settore dell'organizzazione. Ciò anche con riguardo alla componente dati personali.

Paragraph 2 - Analysis of article 25
1a Data Manager (Principle 1. Proactive not Reactive; Preventative not Remedial)
Working according to data protection by design and by default implies increasingly complex skills, especially in relation to the evolution of information and communication technologies.
Considering that data management in general represent an activity with increasing added value in relation to the ability to obtain useful information – for economic operators to exploit it for profit, and for public operators to improve governance aspects and the results of their activity -, it is believed that one of the best practices that could be promoted by the owners is to formalize a data management strategy.
Especially in a complex situation, the (Function of) Data Manager represent the actor who, on behalf of the senior management (of the Controller pursuant to the GDPR), defines the architecture of data resource management in a holistic perspective, he's able to promote a policy to be applied in every sector of the organization (collection, organization, management,

[1] Cfr. https://www.ipc.on.ca/wp%E2%80%90content/uploads/2018/01/pbd.pdf

exploitation, conservation, protection, elimination). This also applies to the personal data component.

Paragrafo 2 - Analisi dell'articolo 25

1b "Ethics by design": la questione algoritmi reti enurali (Principle 1. Proactive not Reactive; Preventative not Remedial; Principle; 2. Privacy as the Default Setting; Principle 3. Privacy Embedded into Design)

Occorrerebbero delle indicazioni specifiche sulla responsabilità dei trattamenti "gestiti" tramite algoritmi elaborati con reti neurali, almeno in considerazione di quanto enunciato dall'art. 13 punto 2 lettera f del GDPR. (cfr anche art. 22, punti 1 e 4)

L'ipotesi dottrinale "provocatoria" di un Titolare e / o di un Responsabile del trattamento interpretata da un robot[2] (macchina neurale) sottolinea l'importanza della questione della massima responsabilità per il trattamento dei dati personali e delle conseguenze per gli individui. Da qui la necessità di approvare regole chiare, sostenibili e inequivocabili sugli algoritmi per la protezione sostanziale dei diritti umani.

In questo senso, la speranza di un'Agenzia europea di intelligenza artificiale è da ritenere sembra degna di una rapida realizzazione.

Paragraph 2 - Analysis of article 25

1b "Design-based ethics": the problem of algorithms and the neural network (Principle 1. Proactive non-reactive; Non-corrective estimate; Principle; 2. Privacy as default; Principle 3. Privacy integrated into the project)

Specific indications on the responsibility of the "managed" treatments must be provided through algorithms developed with neural networks, at least in consideration of the provisions of art. 13 point 2 letter f of the GDPR. (see also art.22, points 1 and 4)

The "provocative" doctrinal hypothesis of a Data Controller and / or Data Processor interpreted by a robot (neural machine) underlines the importance of the question of maximum responsibility for the processing of personal data and of the consequences for individuals. Hence the need to approve clear, sustainable and unequivocal rules on algorithms for the substantial protection of human rights.

In this sense, the hope of a European Artificial Intelligence Agency seems worthy of a rapid realization

.

Punto 11

2. Pseudonimizzazione (Principle 2. Privacy as the Default Setting)

Con riguardo alla pseudonimizzazione, si suggerisce di chiarire – per sgombrare il campo da equivoci – che, attesa la protezione "parziale" dei dati personali rispetto all'anonimizzazione, il ricorso alla stessa dovrebbe trovare motivazione in specifici casi quali:

- segmentazione all'accesso connessa a una gestione per funzioni interne dei dati, dove per i processi che non ne necessitino, si operi solo su dati pseudonimizzati (mentre in altri processi i dati saranno completi e in chiaro);
- utilizzo solo di dati pseudonimizzati e conservazione sicura e tracciata degli elementi di decodifica, laddove il mancato ricorso all'anonimizzazione possa ricorrere da esigenze quali l'aggiornamento dei singoli record.

In ogni caso andrebbero definite apposite regole gestionali per gestire i casi in cui gli elementi autorizzati al trattamento mutino settore operativo all'interno dell'organizzazione (da processi pseudonimizzati a processi in chiaro e viceversa).

[2] F. Pizzetti "Intelligenza artificiale, protezione dei dati personali e regolazione" (Torino, 2018, Giappichelli)

Point 11 2.

2.Pseudonymisation (Principle 2. Privacy as the Default Setting)

As regards pseudonymisation, it is suggested to clarify - to avoid misunderstandings - that, given the "partial" level of protection of personal data compared to anonymization, the use of the same should be motivated in specific cases such as:

- access segmentation connected to management by internal data functions, and for processes that don't need it, only working on pseudonymised data (while in other processes the data will be complete and clear);

- using only pseudonymised data and secure and traced storage of the decoding elements, in which the failure to resort to anonymization could result from needs such as updating the individual registers.

In any case, specific management rules should be defined to manage the cases in which the elements authorized to process may change the operating sector within the organization (from pseudonymised processes to free processes and vice versa).

Punto 22 e Paragrafo 6 Conclusioni e raccomandazioni

3 Trattamento dati e supporti cartaceo (Principle 5. End-to-End Security — Full Lifecycle Protection)

Il trattamento dati avviene sempre più in misura elettronica e i pericoli maggiori per la tutela dei diritti degli interessati richiedono in via prevalente misure di sicurezza di tipo IT e, in maniera collaterale organizzativa.

Resta comunque in essere la gestione su supporto cartaceo di tali dati da gestire anch'essi con appropriate misure di sicurezza. Un rischio da considerare è quello connesso alla fine del ciclo di vita di tali documenti che – se gestito in maniera non appropriata – potrebbe comportare la violazione di dati personali.

Andrebbe promossa l'esplicitazione, in sede di privacy by design e by default, dell'adesione (specificando quale) a "standard formali sui metodi raccomandati per la cancellazione/distruzione per diverse categorie di dati e supporti di dati"; a ciò fa riferimento ad es il documento The DPO Handbook (T4Data) (cfr. nota 330 english version) e l' Opinion 03/2014 on Personal Data Breach Notification – W29 nota 10 (ad es. la DIN 66399 standard di cui non si fa invece cenno nelle nuove Guidelines on Personal data breach notification under Regulation 2016/679 WP250rev.01).

Tali standard si riferiscono anche ai supporti IT (cfr T4Data che menziona: NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization e US National Security Agency/Central Security Service, Media Destruction Guidance).

Point 22 and paragraph 6 Conclusions and recommendations

3 Data Processing and Paper Support (Principle 5. End-to-End Security - Complete Life Cycle Protection)

The data processing is carried out mostly digitally and the major risks for the protection of rights of the interested parties mainly require IT-type security measures, in an organizational collateral way.

However, the paper management of these data needs proper security measures. A risk to be considered is the one related to the end of the life cycle of these documents which, if handled improperly, could result in the violation of personal data.

In the context of privacy by design and by default, the explication of adherence (specifying which) to "formal standards on the recommended methods for deletion / destruction for different categories of data and data carriers" should be promoted; to which it refers, for example,The DPO Handbook (T4Data) document (see note 330 english version) and Opinion 03/2014 on Personal Data Breach Notification - W29 note 10 (e.g. DIN 66399 which is not

mentioned in the new Guidelines on Personal data breach notification under Regulation 2016/679 WP250rev.01).
These standards also refer to IT media (see T4Data which mentions: Special Publication NIST 800-88 Revision 1, Media Sanitation Guidelines and United States National Security Agency / Central Security Service, Media Destruction Guide).

Punto 27
4 Trattamento di dati personali resi manifestamente pubblici dall'interessato (Principles 2. Privacy as the Default Setting, 6. Visibility and Transparency — Keep it Open e 7. Respect for User Privacy — Keep it User-Centric)
Andrebbe chiarito - anche ai fini della privacy by design e by default – come perseguire la compliance al GDPR dell'utilizzo / trattamenti di dati resi noti sul web di iniziativa dagli interessati, ad es reperibili sui social, raccolti anche tramite appositi tool informatici (OSINT).
Se si ritiene che in ogni caso il loro utilizzo configuri un trattamento dati, occorrerebbe chiarire che ogni Titolare che raccolga e si avvalga di tali dati a) censisca un trattamento (ad es "trattamento dati personali disponibili sul web" o "trattamento big data pubblici" e b) provveda anche a definire e rendere nota una apposita informativa, in cui specificare chiaramente aspetti quali: scopo di qualsiasi richiesta di consenso al trasferimento a terzi (e se per lo stesso scopo del trattamento effettuato e se il trasferimento è gratuito o meno), profilazione e relative conseguenze (inclusa la pubblicità su nudge), tempi di conservazione dei dati, ecc.

Point 27
4 Personal data processing manifestly made public by the interested party (Principles 2. Privacy as the Default Setting, 6. Visibility and Transparency - Keep it Open and 7. Respect for User Privacy - Keep it User-Centric)
It should be clarified - also for the purposes of privacy by design and by default - how to pursue the compliance to the GDPR of the use / processing of data made known by the interested parties, e.g. available on social networks, also collected through special IT tools (OSINT).
If in any case their use is considered to constitute data processing, it should be clarified that each Controller who collects and makes use of such data
a) formalizes a treatment (for example "processing of personal data available on the web" or "big data public treatment) " and
b) also define and disclose specific information, in which to clearly specify aspects such as: purpose of any request for consent to transfer to third parties (and whether for the same purpose as the processing carried out and whether the transfer is free or not), profiling and related consequences (including advertising on nudge), times data retention, etc..

Osservazione a margine
La protezione dei dati personali richiede l'impegno di tutti e un'attenta attenzione da parte delle persone a cui i dati si riferiscono.
Inoltre, per consentire ai cittadini di partecipare pienamente alla vita democratica, si ritiene che tutto ciò che riguarda le innovazioni in materia debba poter essere discusso in modo chiaro e diffuso.
A questo proposito, si suggerisce pertanto, per il futuro, che consultazioni analoghe debbano essere condotte mettendo a disposizione dei cittadini dei paesi europei in cui il GDPR è in vigore la consultazione dei testi sottoposti a consultazione democratica nella lingua di ciascun paese.

Marginal observation

The protection of personal data requires everyone's commitment and careful attention by the people to whom the data refer.
Furthermore, in order to allow citizens to participate fully in democratic life, it is believed that anything related to innovations in this area should be able to be discussed clearly and broadly. In this regard, it is therefore suggested, for the future, that similar consultations should be conducted by making available to citizens of the European countries in which the GDPR is in force the consultation of the texts submitted for democratic consultation in the language of each country.

Roma, 16 gennaio 2020