Comments on

- consent, data breach and profiling -

in the GDPR

June 16th, 2017

1. Consent

1.1. Valid consent in practice (free, specific, informed and unambiguous)

Despite unbalanced situations between the data controller and the data subjects, freedom of consent can be ensured if the intended processing is not “unjust”. The consent ground should not be systematically excluded in situations like employment-employee or B2C relationships. Indeed, data controllers can create the conditions for freely given consents (full transparency, openness and time for consideration). In other words, what is relevant is not the existence of an unbalanced situation but **the abuse of this situation**: there should have been both a constraint, a pressure, which has caused the consent to be given and the other party has unduly taken advantage of the situation. The need to comply with laws, regulations and forms of self and co-regulation also provide context for what is reasonable. In addition, the concept of free consent does not oblige organisations to introduce an « a la carte » consent in which the individual can select which aspects of the controller’s activities he/she wishes to consent.

Specific and informed consent requires **clarity of communication** of substantive issues, particularly regarding the purposes of use of data. In this respect Art. 13 GDPR is an **inventory of requirements**, rather than a guide to intelligibility. In order to provide an effective protection, the DPA will need to examine the quality of data protection information provided in each context, rather than checking whether each letter of Art. 13 GDPR has been addressed. The goal is to ensure that the individual understands what the organisation will do with his/her data (smart regulation approach). There should be no uniform definition of specificity in terms of the permitted breadth of consent, since each context is relevant (for instance, as it is recognised in the Regulation (recital 33) in relation to research: it is not possible to anticipate future uses of data at the time of collection and therefore consent for scientific research should be broader than consents obtained in other contexts). In addition, if the consent is extremely specific, there is no room for any **compatible use**, except for those purposes whose compatibility test has already been made by the legislator (ex Art 5.1.b) GDPR), such as the scientific research.

Unambiguous is not necessarily an opt-in; it may be inferred from an affirmative action of an individual, such as to continue engaging with an organisation having been informed beforehand in an effective manner of the organisation’s processing intentions.

1.2. Minors

Art. 8 GDPR raises two issues: (i) the divergence among Member States regarding the age where parental consent is required; and (ii) how to verify the age of an online user and whether the person granting the consent is the actual parent.

An harmonized approach to a child’s consent would be ideal. However, underlying reasons for divergences lie in other local laws which determine the legal capacity to act of children without parental consent, which mainly varies depending on the specific activity (e.g., to get married, to work, to participate in a clinical trial, to assign rights on self-image, to be the titleholder of a bank account or a credit card, etc.). It is true that Art. 8 GDPR only refers to on-line information society services but this concept is extremely broad and will become even broader as the digital society develops.

In an on-line world, and with reference to the question presented in the consultation, the issue would probably only be solved through online identity trust models. Some of them have already been developed in view of the US COPPA (e.g., certification and digital identity trust frameworks, enterprise family identity and permission management platforms and account management and permissioning portals).

1.3. Proof of consent

The proof of consent must be kept during the time a data subject or a DPA may have a claim against the data controller under the GDPR or any other applicable law, which requires the consent to be able to defend the controller's rights. Example (the most simple one): if a data controller obtained a consent to send marketing, it shall keep the consent evidence (e.g., log in, signed form/agreement) until the person withdraws his/her consent and then until the end of statutory period of possible claims (contractual or in tort) that can be brought by the individual, a consumer association or any authority with competence on the subject-matter of the direct marketing at hand.
As a practical point, information on retention periods to the data subjects should refer them to **the principles used** to determine them rather than providing specific details, because the laws that impose retention periods or set forth statutory periods linked to a potential litigation change from time to time (and organisations cannot be obliged to re-do the notices and re-send them each time there is a legal change of this kind).

1.4. Withdrawal

The revocation of consent will not affect the right to **keep and use of the data already collected**. This means that all processing activities (and decisions based thereon) that were made under a valid consent are still valid, i.e., that the withdrawal of the consent has ex nunc effects (no retroactive effects) and not ex tunc effects (from the beginning, as if the consent never existed).
As long as sanctions may be imposed on the controller due to lack of evidence of consent, this duty will prevail over a full removal right to the extent that the relevant statutory periods of these potential claims have not ended.
It is rather customary that a processing activity relies on several legal grounds at the same time. If consent coexists with other legal basis and consent is withdrawn, **the processing activity may continue** as long as these other legal basis still apply to the processing that was the subject-matter of the withdrawal.
If the consent is imposed by sectorial law, as a general rule, a controller will follow the consequences set forth therein regarding the withdrawal, which should **prevail**. For example, in certain EU jurisdictions, if you revoke your authorisation to use an image, you will need to indemnify the organization for the damages caused by your change of decision as any other unilateral early termination of a contract (which is, in general, a breach of contract).

1.5. Consequences of the lack of harmonisation

Local differences in how consent is construed require first to invest significant resources in legal fees to understand the scope and limits of each local interpretation. Depending on the processing purpose, the group may decide to (i) adopt one standard, following the most stringent one (which would entail that the countries with a legal standard less restrictive would be prevented from doing a certain number of activities); (ii) different standards, one per country, which is extremely inefficient in terms of time, cost and future maintenance; (iii) a reasonable common standard (which is not perfect for all the jurisdictions involved but is based on a reasonable risk-based approach). This is not an issue only for multinationals: any SME that wants to be engaged in a global economy is also affected but the situation is even worse because it just does not have the resources to comply. Therefore, any citizen and organisation in the EU very much look forward to a coherent and consistent interpretation of the GDPR among the DPAs.

2. Breach notification

2.1. Who must notify? What is the role of the processor?

The aim of the Regulation is to protect those affected in the event of data breaches from possible detriment of their rights and interests. Processors must therefore notify **without undue delay** to controllers which are responsible to comply with the GDPR's requirements regarding a possible notification of a DPA and affected data subjects. On each processor's side there should therefore exist a process for **detecting infringements** of the controller's instructions or regulations for the protection of personal data and informing the controller immediately. **Damage minimisation measures** should also be part of the processor's procedures to handle data breaches in accordance to instructions of the controller. In order to detect infringements properly it is of pivotal importance to establish a **clear definition** (within a service contract for example) of what is to be understood by "data breach" in the context of service provision.
In any case the DPO both of the controller and the processor must be promptly consulted once a data breach or another incident has occurred (see also WP243 rev.01 p. 14). The final decision regarding the notification of a data breach to a DPA or the data subject though **rests with the controller**.

2.2. Should all data breaches be notified, even if the data are encrypted? When is notification mandatory / not required? Is personal data breach limited to confidentiality breach?

Tokenization, just like encryption, can be considered as an exception to notification to individuals. It is a recognised technique in the UK by the ICO for example, and can provide security if well used (e.g. in PCI DSS standard). Pseudonymisation (as well as tokenization and encryption) should also be taken into account when assessing a data protection breach. For example, if an entity receives sensitive data coded, this coded data can no longer be considered "sensitive", as long as the "conversion chart" is not compromised, In addition, if this company does not have access to the conversion chart, it will be unable to notify the data subjects of the breach since it does not have access to their identity and contact details (but only to coded data). Furthermore, the entity shall not be obliged to **acquire or process additional information** in order to identify the data subject for the sole purpose of complying with this Regulation in that matter according to Art. 11.1 GDPR. Nonetheless this company shall **inform the data controller** of a possible data breach.

2.3. Deadlines for notification

As a data controller needs to be aware of a data breach, it should be made clear that the 72h for the data controller start as of the first notification by the processor.
Regarding relevant stakeholder within procedures for dealing with data breaches the key role of the DPO is not explicit enough in the GDPR. In general, the role of the DPO can be described in three phases:

1) Before an incident that caused a data breach:

a. The DPO ensures a procedure to anticipate a notification obligation by the constitution of a transverse **ad hoc working group** across the organisation. The DPO must prepare his/her organisation to face a possible data breach. It is up to the DPO to create that cross-functional group, combining Chief Security Officer (CSO), Chief Information Officer (CIO), Business, Legal, Communication, Risk Manager, etc.);

b. The DPO ensures that, in the case of an impact assessments that would be carried out by the data controller for the processing operations submitted to him/her, a possible notification has been anticipated. In particular, in order to verify that the consequences of a possible violation for the data subject have been studied and anticipated;
c. The DPO ensures that the principle of privacy by design is taken into account when assessing possible future notification;
d. The DPO can also ensure that the measures referred to in Art. 34.3 (a) are put in place so that the data are made unintelligible (e.g. by implementing state-of-the art encryption technology) in order to reduce the risks for the persons concerned.

2) During the incident that caused a data breach:

a. The data controller informs the DPO of the violation to a processing of personal data. This information must be provided internally to DPO in a **timely manner** according to the principle established in Art. 38.1 GDPR. The DPO must be part of ad hoc working group handling the data breach. The CISO is responsible for all operations aimed at: to objectify (i) the security incident; (ii) its seriousness; (iii) the number of persons involved in the violation, (ii) correct the fact or the situation that led to the occurrence of the violation (iii) to collect any information that identifies the perpetrators and establishes responsibilities. The CISO is the only person authorized to formulate (communicate) internally on these elements. He/she shall inform the DPO as a matter of priority.
b. The DPO, in **full independence** and taking account (i) the possible impact assessment carried out for the processing concerned (analysis or the methodology of which she/he has supervised), (ii) his/her or other remarks included in the documentation of an initial impact assessment and possible reviews of the assessment of the processing concerned, (iii) possible impacts on the persons concerned, (iv) characteristics of the incident giving rise to the infringement, (v) any measures implemented by the organisation to make the personal data concerned unintelligible, (vi) legitimate interests of the data controller, (vii) guidance of the ENISA i.e. regarding the severity of a breach, advises the data controller to notify the supervisory authority: if this action is recommended, the DPO advises the data controller (or data processor) (i) on the deadline and content of the notification, (ii) on notification requirements of data subjects and (iii) on the corrective measures to be taken within the organisation. Final decisions are made by the data controller (or data processor). In any event, if notification to the supervisory authority is not recommended by the DPO (low-severity incident, effective safeguards in place, no risk to persons, etc.), the incident is **duly recorded in detail**, such as in a dedicated chapter of the DPO's annual report, which is available to the supervisory authority.
Throughout the period of notification to the supervisory authority, the DPO acts as **a contact point**. The reference to “other contact point” in Art. 33.3 GDPR is applicable only where there is no DPO.

3) After the incident that caused a data breach:

a. The DPO advises the data controller on the **documentation of** the data breach and related measures and subsequent measures for mitigating risks for the rights and interests of the data subject and keeps track of incidents involving a data breach, treatment by treatment (Art. 33.5 GDPR). The CISO cooperates with the data controller and the DPO to these purposes.
b. The DPO shall ensure that an **a posteriori analysis** is carried out in order to (i) improve data protection measures, (ii) review the privacy impact assessment if necessary, (iii) modify the processing (for example: better data minimisation or enhanced encryption techniques). The CISO conducts this analysis, to which the DPO is associated;

c. The DPO can also ensure that “near misses” are documented as well and operational lessons are learned from their examination.

The assessment and objectification of the severity of the breach should be primarily be made by the DPO or, where appropriate, by automated tools selected with the DPO. Such mechanism makes full use of the **independence** of the DPO, his/her ability to take into account the **context**, **the interests of the data subjects**, and his/her knowledge of the processing concerned. Without diminishing the ability of the supervisory authorities to take cognizance of incidents that have not been notified, this mechanism makes it possible to benefit from the DPO.
Such mechanism can also help the authorities to manage data breach notifications, preventing them of being **overwhelmed by data breach notifications**. In one of its previous positions, the Article 29 Group « recommended that minor breaches be excluded from the notification requirement to avoid burdening data protection authorities (DPAs) unnecessarily ». Similarly, ENISA, in its recommendation, also mentioned: « should a personnel data breach be low of negligible impact no further notification to the competent authority should be required ». The involvement of the DPO will **facilitate the work** of the authorities.
In summary, the DPO should not only be a point of contact, but should be a driving force in this regard: he/she can ensure that the organisation is prepared, that the possibility of an incident which could trigger a notification of a violation is studied in PIA and upstream of any treatment project, s/he can ensure that "appropriate safeguards" are considered to avoid reporting, that lessons learned from incidents are learned, keep up to date the statistics that indicate the most exposed treatments, and so on.

2.4 Data breach vs. freedom of information

Data breaches must be documented by the data controller. This documentation is kept in order to demonstrate compliance when being consulted by DPAs. It should be clarified that this documentation is **not within the scope of the freedom of information legislations** of Member States. It is indeed critical that this information should not be easily accessible to ill-intentioned individuals or organizations.

3. Profiling

3.1. Profiling concept and automated decisions

As per Art. 4.4 GDPR, profiling always entails an automated processing of evaluation (analysis or prediction). However, not all profiling activities will entail the kind of automatic decisions to which Art. 22 GDPR refers, which are only decisions (i) based solely on an automated processing (i.e., with no human intervention); and (ii) which produce legal effects concerning the individual or similarly significantly affects him/her. Only when this kind of decisions are adopted, (i) information to the data subjects on the logic, significance and consequences must be provided (upon collection as per Art. 13/14 or as a result of an access request, as per Art. 15); (ii) a data protection impact assessment must be conducted (Art. 35.3); and (iii) the individual is entitled to obtain human intervention on the part of the controller and contest the decision (unless required by law or a contract).
Profiling activities (irrespective of whether they are linked to this kind of decisions) may entitle the data subject to object thereto (i) with no justification, when related to direct marketing; or (ii) by providing appropriate justification, when related to a processing based on a public interest or a legitimate ground (Art. 21).

Any classification of individuals according to a specific segmentation criteria may be deemed to be a profiling, assuming that it is actually carried out by machines (the GDPR definition requires an "automated" processing), which is not necessarily yet the case in practice (even if the technology may exist). Examples of classifications could be: the students of a class classified per mark to evaluate their performance at class; the sale force, where employees and agents may be classified by sales figures to evaluate their performance at work; patients data to evaluate whether he/she may be eligible to participate in a clinical trial and who are previously classified according to the features that are relevant to the relevant therapy (demographic data, medical data, specific gene alteration, etc.). None of these cases, prima facie, put the individuals' privacy at risk and they all fall under the reasonable expectations of the data subjects. Besides, none of these examples are actually falling under the GDPR "profiling" provisions. The last example, in particular, is indispensable for the clinical trial to have any chance to be successful and protect patients' health conditions.

It seems that the primary issue is not necessarily the profiling itself (the profile generation) but rather **how this profiling is actually used**, i.e., its purpose, its **impact** on the individual and the **lack of human intervention** (the profile application). The attention must therefore first be focused on profiling activities (i) based solely on an automated processing; and (ii) which may produce unfair, adverse and significant effects on the concerned individuals regarding the access to essential services (mortgages, insurances, jobs) or may affect his/her dignity and freedoms. Only when we know the profile application, we may assess whether the profile generation is appropriate.

The rationale of Art. 22 is (i) to protect the interest of the data subject in participating in the making of decisions which are of importance to him/her; (ii) to avoid automatic acceptance of the validity of the decisions reached by a machine and a concomitant reduction in the investigatory and decisional responsibilities of humans in addition to the possibility of machines making mistaken judgments; and (iii) to fight against the threat of alienation and to human dignity and freedom.

Based on the above, there would be no apparent reason to apply article 22 when a decision has **purely beneficial effects** for the data subject but rather when the decision is adverse. Indeed, there exists a large amount of conceptual (and practical) overlap between the notions of "significantly" and "adversely". However, this overlap notwithstanding, the criteria cannot be read as fully commensurate with each other. Some adverse effects can be too trivial to be significant. Indeed, the fact that a decision has adverse effects is a necessary but not a sufficient condition for finding that the decision has significant effects. In addition, fairness does not entail to treat all individuals the same way but to apply different treatment to different situations (students that have different marks could not be treated equally; workers who perform better than others must be rewarded; patients who suffer an illness must be treated accordingly, etc.). Thus, Art. 22 GDPR would apply when a profiling would have an **unfair**, **adverse** and **significant impact**.

3.2. Information to the data subject

In case of the automated decisions to which Art. 22 refers, a DPIA as per Art. 33.5 GDPR is required, which entails that the logic of the software used and other possible risks should have been assessed (as well as the appropriate safeguards, if required). In addition, Arts. 13 (upon direct collection) and 14 (upon indirect collection) require providing information to the data subject. In this regard, detailed information of the software logic would not be required and be counterproductive. To inform the individual that a mathematical or statistical procedure or artificial intelligence technology is used to analyse or predict the relevant features, should be **appropriate to provide meaningful informatio**n on the processing

while protecting the software model as well (protected by IP rights, trade secret rights and contractual confidentiality obligations).

3.3. "Privacy by design and by default" in profiling activities

Ideally, privacy by design would mean, that the instructions introduced by the programmer or how the machine learns through artificial intelligence are documented in a manner that could be interpreted by a human being, in order to prevent or correct inaccuracies that may lead to unfair significant adverse consequences for the individuals. The society shall seek interpretable models that allow humans to intervene and adjust the models used. However, this seems to be easier to state than to achieve and is a current challenge for scientists: http://nautil.us/issue/40/learning/is-artificial-intelligence-permanently-inscrutable

3.4. Limits

Depending on the context, the data protection impact assessment regarding the profiling leading to the decisions under Art. 22 may advise, as safeguard, to exclude certain information from the profiling creation in order to remove or mitigate certain risks.

Bonn,
Den Haag,
Dublin
Madrid,
Paris,
Warszawa,
Wien,

June 16th, 2017

About CEDPO:
CEDPO was founded in September 2011 by European Data Protection Organisations, namely, AFCDP (*Association Française des Correspondants à la Protection des Données à Caractère Personnel*) of France, APEP (*Asociación Profesional Española de Privacidad*) of Spain, GDD (*Gesellschaft für Datenschutz und Datensicherheit*) of Germany, and NGFG (*Nederlands Genootschaap van Functionarissen voor de Gegevensbescherming*) of The Netherlands. The Confederation was soon joined by ADPO (Association of Data Protection Officers) of Ireland, ARGE DATEN of Austria and SABI (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*) of Poland.
CEDPO aims to promote the role of the Data Protection Officer, to provide advice on balanced, practicable, and effective data protection and to contribute to a better harmonisation of data protection law and practices in the EU/EEA.

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu