2017 GDPR Fablab – Results of the discussions

The General Data Protection Regulation (GDPR) officially published on May 4, 2016, will become applicable in all EU Member States on May 25, 2018. We have now reached **a major turning point** having **only approximately one year** to finalize our preparations for its application.

Thanks to the consistent support and cooperation of interested stakeholders, we have been able at the WP29 level, **to produce a number of guidelines** (on DPO, lead authority and data portability) and we have published our draft guidelines on DPIA which are **open for public consultation until May 23rd 2017**.

The WP29 has acknowledged the importance and value of **different stakeholders' operational feedback on the implementation** of the GDPR and is grateful for this fruitful cooperation.

On January 3, 2017, the WP29, as part of its global implementation strategy of the GDPR by 2018, **adopted its second Action Plan for 2017**.

This WP29 action plan complements the 2016 priorities (certification, DPIA, administrative fines, setting up the European Data Protection Board etc.) and **draws new objectives and deliverables for the coming year.**

In order to **prepare for the timely and proper implementation of the GDPR**, the Article 29 Working Party organized a second **Fablab workshop** which took place on April 5 and 6, 2017 in Brussels and enabled participants to discuss with European representatives of the industry, the civil society, academics and relevant associations, certain **operational and practical issues**.

More than **90 participants** were present at the Fablab including representatives from **Data Protection Authorities** (DPAs). Participants **focused on some of the priority issues identified in the 2017 Action Plan of the Working Party**.

The Fablab's objective was to "feed" the Article 29 Working Party in order to develop, at the end of the year, best practices and guidelines with regards to:

(A) the criteria, including practical aspects of a valid **consent**

(B) **data breach notifications** made to DPAs and to data subjects

(C) the criteria and conditions for decisions based on **profiling**

Workshop on Consent

Moderators: Giovanni Buttarelli – European Data Protection Supervisor (EDPS) and David Martin – Senior Legal officer (BEUC)

I. Introduction

The workshop participants discussed the notion of consent mainly established under Articles 4 and 7 of the GDPR.

The discussion started with an overview of the changes provided for in the GDPR on consent. **The general conclusion was that there is more continuity than novelty**, yet there are some important new elements introduced by the GDPR.

The use of **consent as legal basis will be scrutinized more severely, particularly the conditions for valid consent** also in accordance with the principle of accountability.

Currently, **consent is one of the legal grounds for processing**.

In some cases, it might not be the appropriate basis for processing data. Comment on this point, some sectors feel the regulation wants to discourage them from using consent, other consider that too much focus is placed on consent, restricting their choice for legal basis.

II. Call for action to DPAs

- The notions of **"informed" consent** and what does/does not constitute a *"clear affirmative action"* needs to be further explained.
- There is a general uncertainty about **the existing consent or existing declarations on consent.**
- Clarity is also required on the **way to manage consent for more than one purposes** (see recital 32).
- Clarification is required as to what extent consent should be given for every single processing operation or rather to every purpose
- **Children and scientific research** were identified as issues that need specific guidance in particular with regard to the specificity of consent.
- The guidelines should clarify the situation when there are **joint controllers** or cases when one party is collecting consent on behalf of another. How to manage the consent (to give consent but also to withdraw consent) in that situation?
- Guidance is also necessary on the meaning of the words ***"clearly distinguishable"*** in article 7.2. Is it ok to put consent requests in the terms and conditions or not?
- Guidance is also necessary on the practical implications of Article 7.4, how to assess conditionality and its impact on the validity of consent.
- **What makes a freely given, specific, informed and unambiguous consent. Where are the novelties vis a vis 95 Directive**? It was mentioned how important it is to have common understanding of the terminology. Main novelties, the 'clearly distinguishable aspect' and the notion of 'imbalance of power'. Need to 'unbundle' consent from the TCs. Call for clear common understanding on all these elements.
- The need for granularity in terms of the purposes and parties concerned by the consent request.

III. Concerns

Regarding transnational **flow of data**, there is a concern about sharing sensitive data where there is **no equal protection.**

Minors are a priority but resolution lies at MS level and the age **verification of a minor** is problematic. The verification of consent by the holder of parental responsibility is also problematic.

Regarding **research,** there were questions about the consent for the **secondary use of data for research purposes** and about the definition of information society services provided normally for remuneration and whether e.g. online patient services fall under this.

Participants raised the uncertainty about **withdrawn consent and the consequences if the user refuses to give it**. Are "take it or leave it" situations still allowed, if so under which circumstances? What does "without detriment" mean in practice when consent is withdrawn?

A **need for flexibility was presented**, on a future oriented approach regarding to how technology works. **Creativity and technological advancements** need to be taken into account in the drafting of the guidelines. Consent should not lead to a fatigue of the users.

Consent is the most difficult legal ground for processing to prove.

IV. Other specific questions

- Can the data subject give consent to some recipients but not to others?
- How to have and to prove an **oral consent**?
- What about **conditional consent**? (Further explanations are needed on Article 7.4)
- Could conditional consent be valid with regards to sensitive data in the context of the provision of services, such as insurance?
- What if the processing is based on consent and the data subject **withdraws his/her consent** but there is **another legal basis for the processing?** (This has been identified as unfair practice).
- What about the **effects of withdrawal** and the guarantees of **data deletion**?
- Could consent be **indefinite** or do we need to **renew** consent?
- Should there be a **case by case analysis**?
- What **kind of information** has to be given to the data subject? How well identified should the recipients be (link with article 13)?
- What about consent given for processing operations and when this is **reused on other operations?**
- What constitutes a clear **'statement'** a clear affirmative action, is simply clicking on a certain link or continuing using a service for example enough?
- **Interplay of Article 35 about privacy impact assessment and the provisions on consent.** Do you have to take special care with when requesting/managing consent if you have identified a specific risk during the PIA? (e.g. that minors might use your service?)
- Whether it would be ok to have '**recommended settings'** which would still require an affirmative action from the user in order to choose
- What is the meaning of "**clearly distinguishable**" from other matters? Does it refer only to "choice" or "notice and choice"?

Workshop Data breach Notifications

Moderators: Wilbert Tomesen – Vice-Chairman and member of the Dutch Data Protection Authority and Gwendal Le Grand - Head of Technology and Innovation - French Data Protection Authority - CNIL (FR) (CNIL)

I. Introduction

The workshop participants discussed the issues relating to data breach notifications established under Articles 33 and 34 of the GDPR.

Data breach notifications should be seen as a tool to **enhance compliance**.

The participants would be happy to receive a kind of **report** (landscape) on all data breach notifications (anonymized) to get an **overview per sector (+ measures taken)** and learn from each other.

Participants also requested the **consultation of IT professionals** when drafting guidelines on that topic.

Finally, participants think that it would be useful to get guidelines on how to articulate GDPR with other instruments such as the NIS directive.

Participants requested **more flexibility on the content of the notification**.

II. Call for action to DPAs

- There is a dilemma on how to **fulfil obligations** and **avoid reputation issues**
- Procedure for lead authority (who has to be notified)
- Clarification of data breach reporting
- Not to delete certain elements but to **add: some information such as the possibility to name their processor which is responsible for the breach**.
- They also requested the possibility to make an **incomplete notification**.
- Association of risk
- There is a need to define a data breach.
- What to notify?
- Content/ Naming processing that are responsible for data breaches directly to individuals. Difficult to correlate the events (Add info to notification at the authority).
- Common notification form translated in different languages
- Content: not all technical details of the breach/some information is not useful
- Who has to be notified?
- When?
- When are you aware of the breach? Escalating procedure sometimes non-existent. It is important to know **when 72 hrs. start**. Link between notification and security provisions
- Maybe you cannot make a notification with all that is required in legislation/maybe add more information at a later stage: **what about an incomplete notification**.
- Acknowledgement from DPA on receipt of notification
- The reality of data breaches was highlighted because it takes time to understand the breach. The deadline should be 72 hrs. from the point that we understand what the breach is and not when we are aware of the breach.

III. Concerns

Participants take the view that the scope of the term "personal data breach" is often **underestimated**. It is **not only confidentiality breaches**. They ask for a clarification in the guidelines.

The question was raised of **which DPA to notify** in case of different data subjects in different Member States. What if the notification of a breach is forbidden because of a criminal investigation?

Participants also requested guidance on the **72 hrs. deadline and more particularly on the starting point deadline**.

Participants takes the view that DPAs should have a **secure channel** in place for the notification of data breaches.

Impact on reputation

Notification to data subjects: not only number of individuals taken into account we need to provide **guidance on severity of a breach/Tools enabling to assess the severity of the breach.**

SMEs general guidance: best practices on notifications with a contact point within the company.

Participants take the view that **multiple notifications should not be made to multiple authorities.**

V. Other specific questions

- Notification to data subject and requirement to **give information in clear language**
- Use existing **common channel**/Send clear and dedicated notification of data breach
- **Good practices** among the sector
- Justification if you **surpass the 72 hrs. deadline**
- Telecom operators face **different deadlines for notifications**
- High level of **confidentiality**
- Forensic/legal/media people to deal with that
- More specific about how **controller** gets **aware of the breach/and when**
- **Ways to notify?** Mail/Phone etc. Also, controllers should send a message dedicated to the breach - they should not include the notification in some other kind of communication
- **Disproportionate efforts of individual information**. There is no conclusion on that, controller needs to keep evidence of data breach
- Provisions on GDPR and links with other EU legislation/ Useful to explain to have a single organization on notification.

Workshop Profiling

Moderators: Giuseppe Busia – Secretary General - Italian Data Protection Authority and Carl Wiper- Group Manager - Information Commissioner's Office (ICO)

I. Introduction

The workshop participants discussed the issues relating to profiling and automated decision making established under Articles 4 and 22 of the GDPR.

In the GDPR, profiling is considered as a type of processing and its objective is not to outlaw profiling or automated decision-making.

The main elements of the discussion focused on the following:

- Human input into the decision-making process
- Transparency
- Fair processing: ethical decision-making/organizational decision making
- Logic of decision making/ amount of detail to be given to data subjects
- Commercial confidentiality and trade secrets: Purpose of profiling is important /what is the impact: understand the criteria
- Find balance in promoting trust
- Focus on goals.

II. Call for action to DPAs

Article 22 - automated decision-making

- There is no clear distinction between automated decisions and those with **human intervention**. There can be both fully automated decisions whether a decision is solely automated or involves human intervention has to be decided on a case by case basis**.** Some clarity is required in guidance.
- In financial services there are also international guidelines which may be relevant, for example for pre-contractual assessment for prevention of fraud.
- How can an algorithm be made meaningful to a consumer? Controllers need to understand what information they should give to data subjects about algorithms, in order to make the processing meaningful to them.
- Controllers need clarification of the particular situations envisaged in article 22(1)
- The terms **"legal effects"** and **"significantly affects him"** need interpretation. **Significantly affects is risk-based;** it relates to risk and harm. It is not simply a question of whether the effect is positive or negative. The question is, does it have an impact on a right or freedom, for example the right to freedom of expression? If so, then there is a significant impact.
- The individual has a right to object to profiling under Article 21; does the individual also have a right to object under Article 22(3)?
- There is a distinction between profiling as defined in Article 4 and automated decision making under article 22. Guidance is needed on this.

Should there be some limitations to the data that can be used?

- Should some types of data be excluded? If the individual has consented then sensitive data can be processed.
  - The **GDPR harmonizes the rules**; Member States can impose further conditions on certain data, but **they cannot go below those of the GDPR**. The GDPR sets the level. So data that raises ethical issues should not necessarily be excluded. However, controllers may decide to exclude a specific use of data.
  - Should this apply to all sectors? Profiling could be excluded **for certain purposes**.
- What about indirect discrimination for a legitimate purpose?

Transparency information and access rights

- It may be difficult to explain the end use of the profiling. How do controllers provide the right level of detail?
- Controllers need clarity on the term 'meaningful information': does it mean information about the algorithm?
- There is a limit on how transparent controllers can be:
  - Is transparency only achieved through privacy notices and legal notices, or does it also involve educating data subjects?
  - DPAs should be realistic and recognise that transparency requirements can be a burden for controllers.
  - What is the purpose of transparency? Is it about pushing for companies to be accountable?
  - What is the role of the DPO in relation to transparency?
  - The DPA role is important: controllers also have to be transparent to DPAs, particularly because data subjects may not have the ability to understand complex processing.
- The purpose of transparency is to enable people to exercise their rights.
- Transparency is also important to ensure that companies are protecting fundamental rights – for example, are they using illegal data? The public need to know when violations exist.
- Controllers need to be able to understand the algorithms they are using and be able to explain them. But at the point when they have to give the transparency information required under Articles 13 and 14 they may not know what the outcomes of the profiling will be.

III. Concerns

Children: The ethical aspect of profiling was raised in relation to children. How would controllers know whether a person is a child or not? This is a difficult question because of differing national practice on age limits. The guidance should avoid getting into specific issues about age verification.

Purpose of profiling: Profiling is done for two reasons: to track the behavior of individuals, or to understand a problem and find an answer; for example, to understand which employees are most likely to leave a company or to detect patterns of disease.

Profiling is linked to artificial intelligence and machine learning: Sometimes machines make better decisions than people**.**

Accuracy: The need for accuracy is different in different sectors. Businesses may carry out profiling for reasons of profitability, but profitability does not always require accuracy. Profiling is not only about profitability.

Data subject perspective: From the perspective of the data subject it does not matter how profiling is made. The data subject should have access to the inferences that controllers make on the basis of his data. The data subject needs to have the right to know the conclusions that are made about him and the right to object, for example in relation to insurance risk.

Organizational accountability and responsibility: The guidance should make companies think about what they need to do. There is no "one size fits all". Profiling is different in different industry sectors. Sectoral guidance would be helpful.

Profiling is a form of processing of data, so the main principles (minimization etc.) apply. There are many types of profiling.

IV. Additional questions

- Should scoring fall under profiling?
- How realistic is it to use legal obligation as a basis for automated decision making?
- Does any human intervention before or after or during the process mean a decision is not solely automated?
- What if the profiling is created by another party?
- Facial recognition systems are an example of automated decision making. Individuals can object and find out why they are denied access
- Controllers have the responsibility to explain how and why they are profiling. How can they explain the complexity of profiling?
- There is a balance between innovation and regulation to protect data subject interests, but innovation will also bring benefits to the data subject
- Profiling might turn out to be fool's gold
- Does classification constitute profiling? The definition in the GDPR is broad. It is intended to include classification.