# Fablab “GDPR/from concepts to operational toolbox, DIY”- Results of the discussion

The General Data Protection Regulation (GDPR) was officially published on May 4, 2016 and will become applicable on May 25, 2018.

In order to **prepare for the timely and proper implementation of the GDPR**, the Article 29 Working Party organized a **Fablab workshop** with the title “*GDPR/from concepts to operational toolbox, DIY*”, which took place on July 26, 2016 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 40 representatives from **Data Protection Authorities** (DPAs). Participants **focused on the priority issues identified in the Action Plan of the Working Party**, namely, the compliance toolbox aiming at making companies more responsible and accountable and the new right to portability which strengthens citizens’ rights.

**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 delivery of guidelines on the Data Protection Officer ;
(B) the development of guidelines on the format, scope and modalities of Data Portability ;
(C) the production of a methodology and templates for Data Protection Impact Assessment, including the definition of guidance related to risk assessment in the GDPR, and finally ;
(D) the definition of criteria and mechanisms relating to certification and certification bodies.

The Article 29 Working Party should organize another **Fablab workshop in 2017** for the discussion of other important operational and practical issues relating to the GDPR.

## A. Data Protection Officer (DPO)

Moderators: Willem Debeuckelaere - President - Privacy Commission (BE) and Albine Vincent - head of DPO department - French Data Protection Authority - CNIL (FR)

### I. Introduction

The workshop participants discussed the issues relating to the Data Protection Officer (Articles 37, 38 and 39 of the GDPR).

### II. Interpretation of the concepts: (a) "*core activities*" and (b) "*large scale*" " (Article 37.1 (b) and (c))

The group discussed the need for a flexible interpretation of the above concepts, based on the particular facts of each situation (case-by-case basis).

a) Core activities: this concept might be interpreted as referring to the key operations performed to achieve the controller's or processor's goals. For example, HR data processing does not require the hiring of a DPO but if a company develops a more sensitive system such as a location based system – e.g. tracking the trucks for a transportation company – then the company needs to appoint a DPO.

b) Large scale: the interpretation of this concept shall not be based on quantitative criteria (no standard figures shall be established, this should rather be examined on a case-by-case basis). Concrete examples were given in an attempt to generate specific criteria.

Another point raised during the discussion, referred to the fact that although large companies would always appoint a (or a team of) DPO, small and medium size companies (SMEs) might find it more difficult to afford such extra headcount. For that purpose, it was considered, if possible, to provide assistance to SMEs through sectorial associations.

The last point of this discussion concerned the issue of whether a company voluntarily having appointed a DPO, should or not follow all the relevant provisions of the GDPR applicable to DPOs.

### III. Designation of a DPO: Requirements and Incompatibilities

The following points were discussed by the group on this matter:

- The appointment of a part time DPO could be acceptable but with great attention to the risks of conflict of interests and of effective resources;
- The appointment of one single individual or a team of individuals as DPO;
- The appointment of legal entities besides individuals (physical persons) as DPO;
- The expert knowledge (interpreted as sufficient knowledge) with regards to data protection, the professional seniority, language skills and training required for the appointment of a DPO;

- The need for the elaboration of standard contract clauses for the appointment of external DPOs;
- The localization of the DPO and his/her accessibility for the data subject;
- The incompatibility arising from being the DPO and the sole owner of the company at the same time;
- The possible specific national rules with regards to the DPO;
- Cost for SMEs for the fulfillment of the DPO appointment requirements;
- Territoriality: Whether a DPO working in a multinational company should report to the top management established in Europe or elsewhere;
- The nature of the DPO's liability: civil or criminal, this shall probably be determined under national law.

## IV. Conflict of interests

- The issue on the conflict of interests should be looked at on a case by case approach;
- Law firms: clear work agreement, establishment of Chinese walls to avoid conflict of interest; Reflections on DPO working for organizations coming from the same sectors and/or being competitors;
- No involvement should occur with the determination of data processing (purposes and means); the position and role matter more than the title itself;
- Appointment depending sometimes on the culture of each company.

## V. Main duties of the data controller/data processor

The main duty of data controllers and data processors is to guarantee the independence of the DPO, this can be achieved by applying, among others, the following best practices:

- Effectively support and empower the DPO;
- Provide the DPO with a direct connection and access to the top management;
- Authorize the DPO to be included and have a real involvement in all data protection activities;
- Establish a clear and transparent mission statement and annual reporting.

Additional duties of the data controller/data processor:

- Provide to the DPO constant and effective training sessions as well as a professional development program with access to resources relevant to his/her tasks in order to maintain a continuing expertise (IT tools, legal knowledge, IAPP (or equivalent) certifications, courses in Law schools and other faculties at universities, launch of specifical professional schemes, etc.). The cost for SMEs for the abovementioned training tools was also discussed.

- Ensuring that the role of the DPO is not that of a police officer; His/her role should be based on trust and his/her goal should be to come up with solutions. The DPO is not supposed to seize/report the DPA (issue of confidentiality and conflict of interest) but to report to the top management which can then decide on the appropriate action to be taken.

## VI. Interpretation of the term "*monitor compliance*" found in paragraph (b) of Article 39 of the GDPR (not discussed)

## B. Data portability

Moderators: Steve Wood - UK ICO and Joe McNamee – EDRi

### I. Introduction – aims and benefits

The workshop participants discussed the issues relating to data portability established under Article 20 of the GDPR.

Accordingly, the group raised the following issues:

- benefits and legislative intent of including data portability in the GDPR;

- links with competition law, consumer choice and the digital economy;

- the importance of individuals having control over their data and empowerment in the digital economy;

- parallels with number portability in the telecoms sector;

- links with the Payment Services Directive.

There was little dispute about the potential benefits of data portability. The group exchanged views on the existence of three main stakeholders involved in data portability: (i) data controllers, (ii) individual users and (iii) third parties "builders" who want to exploit personal datasets and offer services back to individuals. In addition, a range of examples were cited where data portability may be relevant:

- Data held by ISPs, including log files
- Telemetry data
- Energy data
- Pharmaceutical data
- Market research data
- Data held by online retailers

The group agreed that it would be useful to undertake research in order to highlight successful case studies that reflect the benefits of this new right both for individuals and companies.

### II. General Concerns

Representatives of data controllers raised the following concerns with regards to data portability:

- the range of data that could be covered;

- the underlying costs and burdens;

- the harm caused to intellectual property (e.g. data held by online gaming services)

- some data available to individuals under the right to data portability would not be very useful to individuals; and

- the degree of investment from data controllers in developing compliance programs for data portability. There was acknowledgement that data controllers may want to proactively invest more in certain types of systems that contain the most useful data covered by data portability. Data portability requests for the less popular data could also be dealt with reactively, on a case by case basis. Recital 68 acknowledges that data controllers are not required to adopt technically compatible systems. There is some discretion about where data controllers can invest. Whilst there could be different levels of investment by data controllers in proactive data portability programs, the baseline of legal compliance would be required in all cases.

- need for more research to understand and listen to customers about the types of data they may be most interested in.

Participants noted that not all personal data was covered by data portability – these have to meet the criteria established in paragraphs (a) and (b) of Article 20(1).

### III. Interpretation of the concept "*he or she has provided to a controller*" (Article 20(1))

The interpretation of this concept will most definitely be an important part of the WP29 guidance.
This key issue for all the Fablab participants was analyzed as follows:

- On the one hand, the civil society was concerned that the narrow interpretation of this concept would result to fewer benefits for individuals and on the other hand, data controllers were concerned about the impact of a wide interpretation.

- It was noted that recital 63 of the GDPR provided some further guidance to the general right of access established under Article 15. More specifically, recital 63 states that "*the right of access should not adversely affect the rights and freedoms of others, including trade secrets and intellectual property*…".

- Discussion took place with regards to the boundaries of the '*provided by'* concept – it was agreed that it would clearly cover data published by individuals to social media services. Raw transactional data are likely to be covered. Data generated by Internet of Things (IoT) devices e.g. fitness trackers could also be regarded as data '*provided to a controller*'. A limit could be drawn between raw data and data that has analyzed. There were questions about whether metadata could be covered under this concept; which could depend on the circumstances.

- Some participants raised concerns about member state Courts adopting differing interpretations of the concept.

## IV. Interpretation of the concept "*commonly used and machine readable formats*" (Article 20 (1))

There was consensus among the group that it would be difficult to elaborate guidelines focusing on only one commonly used format. This results from the fact that there might be a need to agree on a range of formats used in different sectors and contexts. However it is important that interoperability is possible between formats. Multi-stakeholder work would be required in order to create an ecosystem of formats that can work in different contexts. There may exist a requirement for 'layers' of standards. Data Protection Authorities (DPAs), standards bodies (e.g. W3c) and sector based trade bodies could all participate in this project. There was discussion about whether a propriety format could fit the definition in Article 20(1) – an open format was more likely to meet this definition.

There was recognition that codes of conduct could play a role in developing guidance on the concept of formats.

## C. Data Protection Impact Assessment (DPIA)/ Risks

Moderators: Giovanni Buttarelli - European Data Protection Supervisor and Gwendal Le Grand – Head of Technology and Innovation - French Data Protection Authority - CNIL (FR)

### I. Introduction

The workshop participants discussed the risks of the Data Protection Impact Assessments established under Article 35 of the GDPR.

Under the GDPR, DPIA is:

- A tool for dynamic compliance

- That contributes to: (i) maintaining security, (ii) reduce the risks, (iii) adopt useful measures, (iv)prevent processing in breach of the law and (v) better implement privacy by design and by default.

- It is a new and important tool, recognized as such by the legislator, since the failure to conduct a DPIA (in cases where it is required) may lead to important sanctions.

- A DPIA is done by the controller and has to be conducted before the processing starts. The prior consultation process (when it is required) also needs to be finalized before the processing starts.

- DPAs are to be individually consulted only in limited cases of high risks. Level of detail to be provided to DPAs: in principle, a reasonable level of documentation is to be kept internally or shared with DPAs

- The regulation provides a list of processings for which a DPIA is required (article 35.3).

- The recitals (e.g. recital 75) also give examples of impacts on data subjects (which can help in the assessment of the severity and likelihood of a risk).

### II. Call for action to DPAs

- Specify the criteria listed in Article 35.3;

- Identify a list of processings to be established by DPAS, in a harmonized way at EU level, for which a DPIA is required to do so under article 35.4, also with regards to existing processings already addressed as compliant by national law;

- Produce clear guidance, without being too prescriptive; according to most participants, a DPIA should be thorough but not too complex, and the analysis should be contextualized also with regard to SMEs and scalability;

- Clarify how to handle a DPIA which has a pan-European dimension (e.g. sending the DPIA only to the lead authority and analyzed just by it?)

### III. Concerns

- Specific concerns may relate to public institutions;

- Many participants highlighted that companies have already implemented processes that are similar to DPIAs in order to assess and manage the risks of processing operations;

- Practical implications of cross border operations;
- Ways to articulate a DPIA together with other data protection requirements;
- Modalities to seek the view in practice of the data subjects and their representatives.

## D. Certification

Moderators: Kirsten Bock – European Privacy Seal - EuroPriSe and Sebastian Meissner - European Privacy Seal - EuroPriSe

### I. Introduction

The workshop participants discussed the requirements of Article 42 and 43 of the GDPR on certification. The discussion was structured along four essential elements of the certification mechanisms.

### II. General: The most relevant model(s) to develop privacy certification mechanisms in the EU

It was generally agreed that a formal distinction between seal, label or marks does not exist (yet). The terms cover the reality of existing schemes and no further distinction e.g. with respect to specific messages is desirable. The term used should transport a clear message to individuals. Any term used should – apart from in connection with the respective mechanism – be used to signify the completion of a successful certification procedure. In this context, the participants also discussed whether a certification should require mere compliance with the law or if it should go beyond that ("compliance+", "quality seal").

Different marks/schemes may be used for different sectors. The pros and cons of one scheme vs several schemes was discussed at length. The value of certification in general might profit from a uniform and well-known European certification scheme (umbrella) guaranteeing the appropriate level of uniform and high standards to generate trust.

### III. Accreditation: Main criteria for accreditation of a certification body

The participants discussed the accreditation procedure in general and the roles and obligations of accreditation and certification bodies as well as the role of the DPAs in the accreditation procedure. It was agreed that there is still some need to clarify the relationship between national accreditation bodies and DPAs.

A broad understanding was reached that the national accreditation bodies (Art. 43.1. (b) GDPR) should be obliged to furnish proof of profound knowledge to evaluate the appropriate level of expertise in relation to data protection. In this respect, great impetus should be put on the "*additional requirements*" (Article 43. 1. (b) GDPR) to be established by the respective supervisory authority which is competent pursuant to Article 55 or 56 of the GDPR. It was agreed that these additional requirements should focus especially to set high standards on the knowledge of data protection and privacy.

Whether a DPA should do both, accredit and certify was subject to controversy. A conflict of interest was identified as impediment.

## IV. Certification Scheme: Main elements for a certification scheme

The participants tried to identify the main aspects of a certification scheme. Apart from the requirements already set out in the GDPR, a common or at least transparent level of evaluation was recommended to be required.

Not only the implementation but also the functioning of controls should be subject to review. However, it should be noted that comparability of evaluation also depends on the performance of the respective evaluators. This topic primarily concerns the technical evaluation of processing operations (e.g., is it sufficient if an evaluator relies on a document review only or should statements that are made in documents such as privacy policies be verified by means of an on-site-audit or other appropriate technical checks).

Data protection certification must have a clear focus on data protection and not be confused with IT security which entails that it is not fully covered by existing ISO norms.

On the whole, certification should be both, meaningful and affordable. Nevertheless, there was no common understanding of what both aspects imply.

## V. Certification Procedure: Effective and meaningful certification procedure

Reliable tools/controls were seen as a major condition for success of a certification procedure. The participants focused on potential threats and recommended to include respective procedures for mitigation.

Finally, the following points of reflection were raised:

- What happens if an accreditor or certifier/evaluator fails?
- What should be the procedure if a certification project fails?
- Should the certifier be required to inform the competent DPA (this could be an obstacle for companies to go for a certification in the first place)?
- What happens if a DPA acts as a certifier and the project fails (potential conflict resulting from DPAs being competent for certification and supervisory tasks)?
- What happens if companies do not stick to what the seal says (is revocation of the seal sufficient or should such misbehavior result in some additional sort of sanction such as an administrative fine – cf. Article 83.4 of the GDPR)?