ARTICLE 29 Data Protection Working Party

Brussels, 11th April 2018

Mr Hans Graux
time.lex CVBA/SCRL
Joseph Stevensstraat 7 rue Joseph Stevens
B-1000 Brussel

Subject: your letter of 7th December 2017 and a new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive

Dear Mr Graux,

The Article 29 Working Party (hereafter "WP29") has received your letter of 7th December 2017 and a new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive.

The WP29 welcomes your effort to write and revise the draft code of conduct with the aim to ensure that individuals feel confident that their data are used appropriately.

In general WP29 is of the opinion that the Code needs to show more added value, particularly through more examples and more indications on what must be done and what is good practice. We would also welcome clarification on the legal status of your consortium and the nature and extent of your representation of the sector.

You should be aware that a revised Code would need to be re-submitted under the GDPR in accordance with the procedure in Article 40. To that end, the WP29 is working on Guidelines on Code of Conducts under the GDPR that the new version of the Code will need to meet. The WP29 guidelines will also set out the agreed procedure for the new European Data Protection Board (EDPB, the replacement organisation for WP29) to review EU wide Codes.

When comparing the new draft to the earlier version, the WP29 finds that many of the comments given in the letter dated 10th April 2017 have not been adhered to or addressed. WP29 advises you to go through that letter and check that you have made the appropriate changes and that you integrate concrete examples and instructions to the controllers and processors of data to ensure that the code of conduct gives added value in accordance with WP13, and the requirements of the GDPR. If you find that a certain comment or suggestion

does not require any revising or amendments it should be explained in an attached memorandum to avoid any confusion.

Below you will find examples of questions and remarks which have not been addressed in the latest version of the Code. This is not an exhaustive list so we advise you to take into account our previous letter when revising the Code. In addition to that there are comments on the latest draft of the Code and suggestions for adjustments or clarifications..

Earlier comments and suggestions which have not been adhered to or addressed

- Sector specific explanation of the applicable legal framework needs to be incorporated in the Code.
- Other compliance issues (e.g. cookies) should be acknowledged.
- The Code needs to be clearer on the roles of the parties involved in processing.
- More details regarding the monitoring process of the code are required
- Generally more details should be provided on the difference between data controllers and processors, in particular, in the case of co-controllership, a single point of contact should be offered to the user.
- Specific comments regarding the necessity to review MEF Mobile Policy Generator and Mobile Privacy Notice Code were not addressed
- The future right to data portability needs to be further elaborated on
- More details and relevant examples on how app developers can integrate "privacy by design" and "privacy by default" in their development process as well as be attentive to legal restrictions relating to retention periods would be needed.
- Security issues where the users would like to allow third parties (e.g. their personal doctors) to access their data require clarification.
- The issue of consent, and explicit consent in connection with the processing of sensitive data, is a key element to ensure that the further processing is fair and lawful. The Code should provide guidance on how this can be expressed by the data subject. A controller may not make a service conditional upon consent, unless the processing is necessary for the service, which WP29 would dispute, might not be the case regarding behavioural advertising.
- Children's consent and different situations in which apps can demonstrate how consent has been given by the guardian need to be addressed specifically.
- Aspects of consent withdrawal (in particular which requirements the third parties need to meet when consent is withdrawn) need to be addressed further.
- A number of comments on the governance have not been followed up on: concrete sanctions and remedies; dispute resolution mechanism; how DPAs/public are informed when the code of conduct is breached; criteria for periodic monitoring; criteria to select panel members of the governance bodies (Independence, expertise and the lack of conflict of interests); number of representatives by sector; financial contributions)

General language of the Code

WP29 appreciates the effort to use a non-legalistic language in the Code to make it more accessible. It must however be taken into account that the Code is supposed to be a guidance for controllers and processors to process data in accordance with the GDPR. If the language in the Code differs too much from the GDPR, it will not provide enough clarification about the GDPR and may even not comply with it. The below example about the scope is one of the many points that would benefit from using GDPR terminology.

The Code states that *"if an app developer does not exercise any control over the processing of personal data through the app and does not use the outcome of the processing – which will commonly be the case if no personal data is ever sent to the app developer or to the app developer or to another third party by the app – then the app developer will in principle not fall directly within the scope of applicability of European data protection law".*

It is unclear what is meant by "exercise any control". We believe the Code should instead refer to the definitions of data controller and data processor and make it clear that an app developer which processes personal data in any way is a controller or processor and thus falls within the scope of applicability of the GDPR.

Further comments regarding the new modifications

The examples provided below are examples of points to be further addressed and are not an exhaustive list.

General structure

We would invite you to integrate "Annex III Explanatory Note" in the rest of the Code. Indeed these points seem to form part of the contents of the Code itself.

Consent

The Code should mention the obligation in article 7 (1) of the GDPR (the data controller should be able to demonstrate a data subject's required consent).

The code does not develop the fact that the consent required in some cases for health data must be explicit. It would have been interesting to develop the difference between "regular" and explicit consent and to give recommendations on this point to app developers.

Research

A point of attention should be drawn to the fact that healthcare research will be ruled mainly by member state legislation.

Disclosing data to third party

We would suggest to add to this paragraph that this is an area where Member States will have discretion to adopt national rules on processing.

Data Breach Notification
In this section, the WP29 is now able to refer the consortium to newly adopted guidelines regarding data breach notification (this is a comment as these Guidelines were not available at the time of submission of the revised Code).Reference will have to be made to these guidelines (WP250, now published) and the Code should be revised accordingly.

Accountability
In the new section on Accountability we note that the text of the GDPR has been quoted in this part and would invite the authors of the Code to indicate where the wording comes from. We would also invite you to revise this section particularly in light of the recent Guidance of the WP 29, WP248 (adopted in April 2017).The framework for the DPIA will need to be further elaborated on. The DPIA is supposed to show the characteristics of the treatment, the risks and the measures adopted. The DPIA needs to allow an analysis of risks and measures adopted to address these risks.

Conclusion
The above points and the points made in the letter of 10th April 2017 encapsulate WP29's general and specific comments on the submitted draft Code.

When revising the draft, please consider carefully what "added value" the code of conduct provides as a whole and, in particular, what specific examples, practical solutions or recommendations you could draw from discussions with stakeholders, to demonstrate why your Code would merit being approved. As highlighted above, please be aware that any new submission would have to take into account the comments that we have made in this Letter and the previous one as well as the new guidelines the WP29 will issue which will provide criteria to submit Codes under the GDPR. When a revised draft will be submitted to a national DPA in accordance with article 40 GDPR we recommend that you also include an explanatory memorandum explaining why certain suggestions and recommendations from the WP29 have not been taken into account.

Sincerely,

On behalf of the Article 29 Working Party

Andrea Jelinek
Chairperson