AMICE contribution to the Article 29 Working Party guidelines on profiling and data breach notifications

AMICE welcomes the opportunity to provide feedback on Article 29 Working Party's guidelines on automated individual decision-making and profiling and guidelines on personal data breach notification. The short deadline consultation has not allowed a sufficient due process.

Guidelines on automated individual decision-making and profiling

- The definition of profiling: we believe that the definition provided in in the guidelines is too broad. As an example of this is the statement on page 7: *"Therefore simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose".* We do not agree with this assessment. The normal identification of a person should not be counted as a profiling.
- 'Legal' or 'similarly significant' effects: the terms 'legal' or 'similarly significant' effects are interpreted too broadly when it comes to marketing practices and thus, the guidelines set too high conditions for profiling in the case where it is *"necessary for the performance of or entering into a contract"*
    - The profiling should be legitimate if one of the conditions presented in the bullet points on page 12 is met. Now it states that *"these considerations alone are not always sufficient to show that this type of processing is necessary under Article 22(2)(a) for entering into, or performance of, a contract."*
    - The example in the box on page 20 is problematic as well, because it questions the necessity of the profiling.
    - We believe that the conditions set out on page 25 are quite demanding for the controller: "*The controller would also need to prove that:*
        - *the impact on data subjects is limited to the minimum necessary to meet the particular objective (i.e. the profiling is the least intrusive way to achieve this); and*
        - *the objective is critical for the organisation.*"
- The meaningful information about the "logic involved" is very problematic because the guidelines require very detailed information about the logic involved. Telling the data subject about the criteria relied on in reaching the decision would mean that at the same time the controller should disclose its business secrets.
    - e.g. example on page 14
    - e.g. example on page 15 *"It uses graphics to give tips on how to improve these habits and consequently how to lower insurance premiums."*

Guidelines on personal data breach notification

- The definition of personal data breach is very broad. It is questionable if the "availability breach" should be counted as a personal data breach. We understand that in the context of a hospital, the availability of critical medical data could present a risk to individuals' rights and freedoms. However, this is not the case in many other industries (such as insurance). All of the service breaks or loss of access are not critical and this type of data breach category should be limited only to the health care industry.

- Processors obligations: The guidelines state on page 11 that *"The controller uses the processor to achieve its purpose; therefore, in principle, the controller should be considered as "aware" once the processor has become aware."* This interpretation is wrong; the controller is "aware" after the processor has made an official notification to the controller "without undue delay" according to the GDPR Regulation.
- Accountability and record keeping: the guidelines do not specify the retention period of these documents relating to data breaches.