iLINC Legal & Technology Briefs

Start-Ups And Data Protection – Consumer Consent

iLINC
ICT Law Incubators Network

Start-ups often consider data to be the raw material for innovation. Many start-ups process data they have collected from their end-users. In order to protect the data subject however, start-ups must have a legitimate basis to perform these processing acts. Considering the importance of consumer trust, start-ups may want to obtain consent from their end-users for these activities. Indeed, using consent as the basis for processing activities, ensures transparency towards the end-user, as he himself will have to decide whether or not he is okay with the processing activity. The purpose of this legal brief is to give an overview of the application of consent as a ground for the processing of personal data.

Introduction

Art. 8 of the European Charter of Fundamental Rights states that everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Article 8 of the Charter thus specifically recognises consent as a key condition for the protection of personal data.

Under the EU Data Protection Directive 95/46/EC (DPD) 'personal data' are defined as "information relating to an identified or identifiable natural person" (Article 2 (a)). This relates to information about a person whose identity is either manifestly clear or can be discovered by acquiring additional information.[1] Hence, Article 1 DPD aims to protect the right to privacy of natural persons with respect to the processing of personal data.

Article 2 (d) DPD defines a data controller as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data [...]". The controller will have to comply with the substantial provisions of the Directive as he is responsible for the processing. The definition has two main elements. First, the DPD references a determinative influence ('determines') of each data controller. This natural or legal person decides why certain data is being processed and how this objective shall be reached.[2] This element already links to the second component. The controller determines the means and purpose(s) of the processing. Any data controller may be required to satisfy the consent requirement, as outlined in this legal brief.

Start-ups relying on a business model focused on the processing of personal data for commercial purposes will often rely on consent as a ground of personal data processing. This brief will first outline the concept of consent as it is found in the Data Protection legislation. Following this introductory analysis, the brief will highlight the application of consent in relation to the use of cookies.

Directive 95/46/EC

Article 2 (h) of the Data Protection Directive defines consent as ""any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". The definition can be broken into three elements:

- Specific: Consent should be intelligible and refer precisely to a well-defined, concrete situation of data processing. It cannot relate to a non-exhaustive set of processing activities.
- Freely given: Consent is freely given as long as the data subject is able to exercise a real choice without risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.
- Informed: Articles 10 and 11 DPD provide information requirements for the controller. 'Informed' consent means consent by the data subject based upon an appreciation and understanding of the facts and implications of an action.

The consent definition is further supplemented by Article 7 (a) which specifies the application of consent as a ground legitimising personal data processing. It states that personal data may be processed if "the data subject has unambiguously given his consent." For consent to be unambiguous, the procedure to seek and to give consent must leave no doubt as to the data subject's intention to deliver consent. There can be no room for ambiguity or reasonable doubt. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller. The expression of consent should therefore either be on the basis of an express action carried out by the individual or by being clearly inferred from an action carried out by an individual.

Accordingly, unambiguous consent is required for personal data processing. However, in relation to the special categories of personal data (sensitive personal data), the consent requirement is even stricter. Article 8 DPD contains a detailed regime for the processing of these sensitive categories of personal data. The general rule of this provision prohibits the processing of personal data

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[3] The legislator has however foreseen certain limited grounds under which the processing of sensitive data is allowed, including where:

> "(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent."

Recital 32 of the Directive further emphasises that data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject has given their explicit consent. However, this explicit consent is currently solely required with regard to the processing of sensitive data.

The Proposed General Data Protection Regulation (GDPR) goes one step further and requires that consent given in a written declaration must be distinguishable from any other matter dealt with in the declaration. Safeguards should further ensure that the data subject is aware that, and to what extent, consent is given. The Regulation also stipulates that consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller (e.g. in an employment relationship). Where consent is withdrawn, the data controller must cease processing unless he has an alternative ground to justify the processing, such as for the performance of a contract.

Cookies and the e-Privacy Directive

It should be noted that there is a separate regime applicable in relation to the use of cookies. This is provided by the e-Privacy Directive 2002/58/EC (ePD), as updated by the Citizens' Rights Directive 2009/136/EC. Indeed, Article 5 (3) specifies that informed prior consent is required before information is stored, or access is gained to information already stored in the terminal equipment of a subscriber or user. The subscriber or user must have given his or her consent, having been provided with clear and comprehensive information in accordance with DPD, *inter alia,* about the purposes of the processing. As per Article 2 (f) ePD, consent relies on the definition provided in Article 2(h) DPD (as defined *supra*). However, it should be observed that this consent requirement in relation to cookie use excludes certain types of cookies from the scope of application. Functional cookies are generally exempt from the legal obligations under the framework, unless they are used for tracking or profiling purposes (see Recital 66 ePD).

The Article 29 Data Protection Working Party, an expert advisory organ providing guidelines with relation to the interpretation of EU data protection legislation, has observed that consent via default browser settings is unlikely to be sufficient. This appears to exclude the possibility for implicit consent. Indeed, it is difficult to avoid the opt-in requirement in relation to the use of profiling and/or tracking cookies. Accordingly, unambiguous consent is also required for the placing and/or use of tracking and profiling cookies.

Conclusion

From the above, it is clear that start-ups have a number of requirements which must be fulfilled in order to rely on consent as a basis for the processing of personal data. As many services and applications rely on the processing of personal data, consent is likely to be a key ground for start-ups legitimising their business operations.

The proposed changes in the GDPR will expand the requirement for explicit consent to all personal data processing operations. This will entail more stringent requirements so entities processing personal data should be aware of these legal developments. In conclusion, start-ups should be aware of the requirements laid down in data protection law and the important role that consent plays in legitimising personal data processing.

References

1. Council of Europe, European Agency for Fundamental Rights, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union, 2014

2. Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"

3. Directive 95/46/EC

ILINC is the European Network of Law Incubators. Its main objective is to facilitate the provision of free legal support to start-ups while, at the same time, offering postgraduate law students the opportunity to engage in professional practice in the fast-moving and highly exciting world of technology start-ups.

Visit us on our website:

https://www.ilincnetwork.eu/

Our core partners: