iLINC Legal & Technology Briefs

User profiling under the EU Data Protection Rules

iLINC
ICT Law Incubators Network

Understanding one's customers is the key of any successful business that focuses on providing personalised and targeted services. Start-ups are not an exception in this regard. Indeed, establishing customers' profiles, or in other words "profiling", may play an intrinsic role in a business plan of a new endeavour. It can even help to improve services as well as the overall performance of the company. While an easy access to increasingly sophisticated data mining systems and cheap data storage make the profiling an attractive option for business, it should be noted that this practice is subject to the EU data protection framework, consisting of the EU Data Protection Directive and the E-privacy Directive. This brief will provide guidance on the applicable legal framework for the profiling activities. ILINC recommends this brief to be read in tandem with the iLINC Legal & Technology brief concerning consumer consent.

I. The concept of profiling

In general, **"profiling" implies the collection of data about somebody or something that subsequently can allow to provide a detailed description of a person or a thing.** In the online context "profiling" is understood as a collection of data (e.g., via cookies or device fingerprint) which leads to "a description of a customer or set of customers that includes demographic, geographic, and psychographic characteristics, as well as buying patterns, creditworthiness, and purchase history".[1] For example, Amazon keeps good track of customers' purchasing behaviour, which allows them to intelligently push content to their consumers, such as movie or book recommendations. In this particular instance, a profile has been made based upon the customer's purchasing history and this allows the undertaking to push targeted advertising in an effort to increase sales.

It can be argued that by far the most elaborate definition of "profiling" is provided by the Council of Europe. According to this definition, "profiling" is "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".[2]

II. Why profiling is the processing of personal data?

Profiling essentially entails placing and retrieving information through a cookie or similar device on the customers' device and in this way monitoring users' online behaviour. Though at first sight information obtained in this way may not seem to be personal (e.g., time spent on a webpage), in connection to other information (e.g., IP address), it allows to establish a direct or an indirect link to an identified or identifiable person, and thus, it qualifies as personal data under the EU Data Protection Directive (DPD).[3]

Types of profiles

A start-up may decide to build user profiles for different purposes. Profiles may include but are not limited to the following types:

1. **Predictive profiles** are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on;

2. **Explicit profiles** are created from personal data that data subjects themselves provide to a web service, such as by registering.

3. **Mixed profiles,** which may include online surfing information as well as information entered into a certain application. [4]

4. **Other types of profiles** can be established. For example on the basis of the targeted audience, profiles may be divided into individual and group profiles.

III. Applicable legal framework

Although neither **the EU Data Protection Directive nor the E-privacy Directive include an explicit reference to "profiling", they set the framework for the profiling activities.** The EU Data Protection Directive applies to **"the processing of personal data wholly or partly by automatic means"**.[3] Building user profiles entails processing of data related to a user, which is regarded as personal data. Thus the DPD is applicable to profiling activities. The term **"processing"** is a broad notion and, in the context of the DPD, it may refer to any operation performed on the personal data, including collection, recording, organization, storage, adaptation or alteration, retrieval, use, disclosure by transmission, alignment or combination, blocking, or erasure.[3]

A start-up defining the purpose and means of profiling (e.g., users' data are collected via cookies in order to provide relevant advertisements) would be the **controller** within the meaning of the DPD. According to Article 2 (d) of the DPD, a data controller is "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 [...]".

Noteworthy, **the controller carries responsibility for ensuring compliance with the requirement and obligations set in the DPD.** The main obligations include, providing an **information** notice to data subjects, ensuring **data quality** principles, **determining the legitimate ground for the processing**, (if required) submitting a notification to the national data protection authority, and **ensuring security and integrity** of the **collected personal data.**

While the EU DPD has a general scope, **the E-privacy Directive is applicable to the processing of personal data and the protection of privacy in the electronic communications sector. The E-privacy Directive protects the confidentiality of communications.**[5] Article 5(3) allows only a conditional use of cookies or similar devices that would include storing of information, or gaining of access to information already stored, in the terminal equipment of a user.[6] The data controller (in this context, a start-up) would have to provide a user with an information notice, which would contain the purposes of profiling, and it would have to obtain user's consent for these actions. Note, **the directive does not require to obtain the user's consent for the use cookies or similar devices in the situations:**

1) Where they are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or

2) When they are strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[6]

Consent requirements

Article 2 (h) of the EU DPD 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". For unambiguous consent to be valid, it has to fulfil the following three criteria:

- **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.

Note that in case the processing entails special categories of data an explicit consent is required.

IV. Profiling under Directive 95/46/EC

Prior to launching profiling activities, the controller (i.e., a start-up) should consider requirements set forth in Articles 12 and 15 of the EU DPD.
According to Article 12, **data subjects have the right to obtain from controllers "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred".** This means that in case, the controller needs to inform the data subject about intentions to create a profile (prior or) at the time of the data collection. This could be done via the information notice.

Article 15 of the EU DPD concerns the "automated individual decisions" and allows profiling in two situations. More specifically, the article foresees, that automated decision making (e.g., profiling) can be done:

1) If the decision is taken in the course of **the entering into or performance of a contract**, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

2) If the controller is **authorized by a law** to lay down measures to safeguard the data subject's legitimate interests.

The right to object

Noteworthy, Article 15 introduces a general right for data subjects to object profiling. In particular, Article 15 stipulates that every data subject has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him".

V. Profiling in the near future

The current EU data protection framework will be repealed and modernised by the General Data

Protection Regulation (GDPR or Regulation). The Regulation further specifies and strengthens the data subject's right to object to profiling (Article 19). Article 20 of the Regulation broadens the scope of the DPD Article 15 as it allows to profile users, only after having received their consent to such action. (Article 20.1 (c)).

The Regulation prohibits profiling on the basis of the special categories of data that may include personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures.[7]

VI. Conclusion

Start-ups that intend to engage into profiling for one or another purpose should consult national laws implementing the above analysed directives, namely the EU Data Protection Directive and E-privacy Directive. Moreover, once the data regulation is adopted, profiling activities will become subject to higher scrutiny.

However, and regardless of the regulatory framework or the legality of profiling, businesses should be wary **that a majority of people in the EU (53%) are uncomfortable about Internet companies using their personal information to tailor advertisements**.[8] Therefore, in case of opting in for profiling activities and measures, start-ups should still aim at retaining users' trust. This could be done through developing and implementing transparent policies and accountability measures.

References

1. http://www.businessdictionary.com.

2. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Appendix to Recommendation CM/Rec(2010)13.

3. Council Directive (EC) 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281.

4. Article 29 Working Party Opinion on Online Behavioural Advertising.

5. Directive 2002/58/EC.

6. Directive 2009/136/EC updating Directive 2002/58/EC.

7. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD).

8. Special Eurobarometer 431, Data Protection Report, June 2015.

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: