iLINC Policy Briefs

Start-ups and Data Protection – Purpose Specification & Limitation

iLINC
ICT Law Incubators Network

Start-ups often face the challenge of meeting two fundamental requirements provided for by European data protection law. First, the requirement to specify the purpose of their processing operations the moment personal data is collected by them ('purpose specification'); and, second, the requirement that the collected data must not be processed further in a way that is incompatible with the initially specified purpose ('purpose limitation').[1] In particular, Start-ups have difficulties specifying the purpose because they often do not know their final product or service (and sometimes have not even finished their business model) when they commence collecting data. This brief thus focuses on the criteria, which assist start-ups to comply with the two requirements as well as comply with specific regulation instruments transposing these requirements in the private sector and, simultaneously, meeting a need for openness toward innovation as well as legal certainty.*

By Maximilian von Grafenstein

Purpose specification and limitation between openness to innovation and legal certainty

The determination of purposes being legally relevant and how precisely relevant purposes must or, vice versa, how broadly they may be specified is of the highest relevance, not only for the data controller, but also for the individual concerned. On the one hand, the broader the purpose may be specified, the fewer the principle of purpose limitation restrains the scope of action from the side of the controller in relation to the data. On the other hand, the principle of purpose specification shall enable, in particular, individuals to estimate their risks caused by the processing of data related to them. The principle of purpose limitation shall exclude potential risks that the individuals could not foresee on the basis of the purposes specified.[2] Both principles must therefore balance the opposing interests of data controllers and the individuals concerned.

Despite the importance of these principles, there is almost no reliable criteria that helps to determine the purposes and their compatibility. This leads to legal uncertainty for both data controllers and individuals concerned. Data controllers cannot be sure whether or not their specified purposes meet the principle of purpose specification and to what extent they are allowed to process the data. The individuals concerned cannot estimate their risks because they are often overwhelmed by either too specific or too broad purposes.

Purpose specification is determined by all fundamental rights and not only by Art. 7 ECFR

One reason for this legal uncertainty is the unclear concept of protection of the right to privacy and the right to data protection under Article 7 and 8 European Charter of Fundamental Rights. So long as both rights commonly refer to the term 'personal data' as the exclusive reference determining the scope of application, they pose a risk to substitute the other, more specific, fundamental rights.

The reason for the broadness of scope of application is that social interaction is progressively based on the processing of personal data - in the course of increasing digitization. For example, while decisions concerning an employee previously fell under the right to engage in work provided for by Article 15 ECFR or leading to discrimination possibly infringed the right of non-discrimination in Article 21 ECFR, these decisions today are increasingly based on data processing that falls under the right to privacy and data protection under Article 7 and 8 ECFR. This leads to the situation that the diversity of risks of social interaction is less and less covered by the variety of specific fundamental rights of freedom and equality but instead under one single (common) fundamental right of privacy and data protection.[2]

In practice, this unclear concept of protection results in a unclear situation where neither data controllers nor the individuals concerned are able to appropriately estimate the divergence of risks caused by the ubiquity of data processing and, consequently, answer the question of how to specify or understand the related purposes.

One essential step for the solution of this problem is to consider the right to data protection in Article 8 ECFR not as exclusively connected with the right to privacy under Article 7 ECFR but also as serving to protect the other fundamental rights. In doing so, the other fundamental rights serve, vice versa, beside the right to privacy under Article 7 ECFR, as the legal scale in order to assess the risks of the specific data processing.[3] The substantial guarantees provided for by all fundamental rights specifically endangered by the processing consequently determines which of the purposes are legally relevant and how precisely they must or how broadly they may be specified.

Consent as a (dynamic) protection instrument

The consent given by the individual concerned is a protection instrument transposing the principles of

purpose specification and purpose limitation on the private private sector. Even if the consent equally exists beside any other legitimate basis provided for by law, in practice it often plays a predominant role. In light of this, there should be three particular aspects stressed in this brief:

First, many legal scholars consider consent invalid as a whole if the purposes specified in it are too broad or vague.[4] Such a consideration leads to the uncertain situation where any further data processing based on the consent might be seen as illegal, irrespective of the degree of risk caused by the specific data processing operation. In light of the fact that data controllers, particularly, start-ups are not able to pre-determine all possible future purposes, such an understanding unnecessarily conflicts with the start-ups' need for openness toward innovation. The reason is that such an understanding primarily focuses on the moment the personal data is collected, instead of restraining the scope of action of data controllers at a later stage in order to protect the individuals concerned.

Therefore, instead of considering the given consent invalid as a whole, it would be more effective to take the specific purpose provided for by the consent as starting point in order to determine, in light of the circumstances of the particular case, which data processing is covered by this purpose and which processing is not. A data processing operation which only slightly endangers specific fundamental rights of individuals allows broader purposes than operations, which bear higher risks for the individuals' rights of privacy, freedom or equality.

Second, the dynamic understanding of the legal effects of purposes specified in the individual's consent is flexible and thus fits the need for open innovation processes, particularly, in relation to startups. However, with respect to the requirement of 'purpose limitation', **using the consent as a basis for the data processing also leads to restrictions!** As mentioned above, on the European level, purpose limitation does not require the identity of the initial purpose and the purpose of the further data processing (but only that it is not incompatible). In contrast, once the purpose is specified within the consent form, it is likely that there is no room left to change purposes in this regard. The reason for this is that the consent is mainly considered as a contractual or quasi-contractual agreement between the data controller and the individual concerned. Such an agreement does, in principal, not allow that one party unilaterally deviates from what is agreed upon.[5] If the data controller uses the consent, thus, it is strictly bound to the purposes specified in the consent.

In summary, even if the dynamic understanding of the legal effects of a purpose specified in the consent gives flexibility, it principally is more restrictive than a legal provision authorizing the data processing. These considerations imply that authorizing legal provisions not only allow purpose compatibility (instead of strict purpose identity) but also that this compatibility assessment does in general apply to all stages of the data processing and does not primarily focuse on the moment the data is collected.

Standardized purposes providing for legal certainty

In any case, as long as data controllers, such as start-ups, have to specify their purposes on a case-by-case basis, neither the individual's consent nor another legitimate basis provide for sufficient legal certainty. The reason for this is that individuals have to verify, again and again, what data controllers want to actually do in light of the purposes they have specified. **Vice versa, data controllers must determine, time and time again, how to formulate their purposes and whether their further data processing operations are compatible with those purposes** or not. This situation does not only overwhelm the individuals concerned, but also **hinders data controllers, in particular, start-ups to set up lean and scalable processes.**

One solution for this lack of legal certainty can be to standardize and certify, at least, most common purposes. The reasoning behind this idea is that standards not only serve, in practice, to enhance technical interoperability but also trust amongst parties. **Users of standards can trust that certain criteria are met, given the requirements (control and sanction mechanisms included) of the standardization and certification process.** Such procedures should be **adapted to the needs of data controllers and individuals in order to set up standards and certificates for purposes of data processing.** The same is possible for the tests of purpose compatibility being frequently applied in practice.

On the basis of such standards, it is even possible to implement those purposes on a technical level by means of privacy-by-design. Standardization of purposes means that the **purposes are sufficiently formalized in order to leave their application up to machines.** In the future, individuals could thus set up via their personal devices by default which kind of processing for which purposes they consent to. **Such a kind of consent** would not appear in written form (with hundreds of legal clauses) but **could visualize the stream of data and its meaning in a form that individuals can intuitively understand.**

Policy recommendations for the General Data Protection Regulation

Considering current regulatory efforts towards the adoption of a general data protection regulation, this policy brief – and unlike other briefs produced by the iLINC network - suggests concrete, textual recommendations for the proposed regulation. In light of the above analysis, this policy brief recommends the following changes - highlighted in green - in the text of the General Data Protection Regulation (GDPR).[6]:

Article 1 – Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects (…) fundamental rights **of privacy,** freedom **and equality** of natural persons **by guaranteeing their** right to the protection of personal data.

Recital 25:

Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement or by a clear affirmative action by the data subject signifying his or her agreement to personal data relating to him or her being processed. This could include ticking a box when visiting an Internet website or any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Where it is technically feasible and effective, the data subject's consent to processing may be given by using the appropriate settings of a browser or other application. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. **The determination of the purpose should refer to the context of later data processing with respect to its risks for (the execution of) his or her fundamental rights of privacy, freedom or equality.** If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Recital 30:

Any processing of personal data should be lawful and fair. It should be transparent for the individuals that personal data concerning them are collected, used, consulted or otherwise processed and to which extent the data are processed or will be processed. The principle of transparency requires that any information and communication relating to the processing of those data should be easily accessible and easy to understand, and that clear and plain language **and/or visual representation** is used. This concerns in particular the information of the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the individuals concerned and their right to get confirmation and communication of personal data being processed concerning them. (…)

Recital 41:

Personal data which are, **be it at the time of their collection or any later phase of processing,** by their nature, particularly sensitive (…) in relation to fundamental rights **of privacy,** freedom **or equality,** deserve specific protection as the context of their processing may create important risks for the fundamental rights **of privacy,** freedom **or equality**. These data should also (…)

Recital 46:

The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language **and/or visual representation** is used. This information could be provided in electronic form, for example, when addressed to the public, through a website. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed (…) to a child, should be in such a clear and plain language that the child can easily understand.

Recital 49:

The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, **or, where the processing of data subsequently**

causes a risk for the individual's fundamental rights of privacy, freedom or equality, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. Where the origin of the data could not be provided to the data subject because various sources have been used, the information should be provided in a general manner.

References

* This policy brief was contributed by Maximilian von Grafenstein LL.M. (Alexander von Humboldt Institute for Internet and Society).

1. Article 6 cip. 1 lit. b of the Data Protection Directive 95/46/EC as well as Article 5 cif. 1 lit. a of the draft of the GDPR by the Council of the European Union (version from the 14th of December 2014).

2. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, p. 11.

3. Schulz/v. Grafenstein, The right to be forgotten in data protection law: a search for the concept of protection, not yet published.

4. Explicitly for the German level, Kramer, BDSG Bundesdatenschutzgesetz und Nebengesetze, Carl Heymanns Verlag, 2014 Wolters Kluwer with further references to Gola/Schomerus, ibid., § 4a cip. 22; Plath, ibid., § 4a cip. 29; OLG Köln, decision from the 17th of June 2011 (6 U 8/11); similarly for the European level Dammann/Simitis, EG-Datenschutzrichtlinie, Nomos Verlagsgesellschaft, 1997 Baden-Baden, cip. 7.

5. For example, with respect to the German level, Rogosch, Die Einwilligung im Datenschutzrecht, Nomos Verlag 2013, Seite 36 ff, or Buchner, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006, S. 231 ff.

6. Draft of the GDPR by the Council of the European Union (version from the 14th of December 2014).

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:

HANS-BREDOW-INSTITUT for Media Research at the University of Hamburg

Queen Mary University of London

IViR

iMinds KU LEUVEN