Editorial

There are three main provisions in the General Data Protection Regulation (GDPR) that contain references (directly or indirectly) to the interests of different parties involved with or affected by data processing activities. There are the grounds for legitimate data processing (Article 6 GDPR), the grounds for legitimate processing of sensitive data (Article 9 GDPR) and the grounds that can legitimate the incidental transfer of personal data to countries outside the EU when there is no adequacy decision and there are no appropriate safeguards (Article 49 GDPR). These provisions include references to four distinct interests.

The first possibility is that the data processing (of ordinary or sensitive data) or the transfer serves the interest of the data subject. This will be the case in three types of situations:

1. The data subject consents to the data processing. This ground is based on the liberal/capitalist presumption that as long as the individual is provided with sufficient information, he can decide what is in his best interest. This ground is present in all of the three articles: 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes' (Article 6.1(a) GDPR); 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes […]' (Article 9.2(a) GDPR); 'the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject […]' (Article 49.1(a) GDPR). A special case is present in Article 9: 'processing relates to personal data which are manifestly made public by the data subject' (Article 9.2(e) GDPR). Here, the data subject has consented to (or rather initiated) the data being published (eg making public that one is gay, has a certain health condition, etc) and the presumption is that – when this was voluntary – he will be fine with others using that information.

2. The data subject has signed a contract. This ground is based on the same philosophy as consent, but entails a second step. If the data subject is fully informed, he can reasonably conclude contracts that serve his own interest. If that is the case, the data controller may process personal data for the purposes of that contract; there is a form of implicit or indirect consent. Again, this ground is contained in all three articles: 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract' (Article 6.1(b) GDPR). The same is essentially held with respect to the transfer of personal data (Article 49.1(b) GDPR). With respect to sensitive data, this ground is conditionalised. The parties that the data subject has signed a contract with are limited to those that the data subject can expect will need to

DOI: 10.21552/edpl/2018/2/3

process sensitive personal data, namely a 'not-for-profit body with a political, philosophical, religious or trade union aim' (Article 9.2(d) GDPR).

3. The data subject has not consented directly or indirectly to the processing of personal data, but still the data controller believes that the data processing is in the vital interest of the data subject, such as interests concerning his health. Processing personal data is deemed legitimate when 'processing is necessary in order to protect the vital interests of the data subject or of another natural person' (Article 6.1(d) GDPR). With regard to processing sensitive data and the transfer of data, it is underlined specifically that this ground only applies when the data subject is legally or physically incapable of giving consent, confirming the principle that only the data subject can decide what is in his own interest (Article 9.2(c) GDPR; Article 49.1(f) GDPR). A special situation is mentioned with respect to the transfer of personal data, which may be deemed legitimate when 'the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person' (Article 49.1c GDPR).

Second is the possibility that the data processing is in the interest of the data controller. Obviously, the data processing in the interest of the data subject will normally also be in the interest of the data controller, as the consumer pays for it or gets something else in return. This may not per sé be the case when data are processed in the vital interest of the data subject. In addition, the data controller may process data about the data subject when this is not in the interest of the data subject, but in his own interest. Article 6 stresses that data processing will be deemed legitimate when 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child' (Article 6.1(f) GDPR). This ground can only be invoked by private organisations and not by public ones; the idea being that public organisations only process data when this is in the public interest (not when there are so called 'reasons of state'). Interesting is that this ground cannot be invoked with respect to sensitive data; sensitive data may be processed to protect the interests of the data subject and the public interest (and potentially even the interests of third parties, as will be explained below), but not in the interests of the data controller alone. With respect to the transfer of data, however, this is a possibility (Article 49 lid 1 second indent GDPR).

Third is the situation in which the data processing is in the interest of a third party. This may run in two ways. First, (as stressed in Article 6.1(d) GDPR; Article 9.2(c) GDPR; Article 49.1(f) GDPR) – personal data may be processed without the consent of the data subject when it is either in his vital interest or in the vital interests of a third party. For example, the personal data of a mother (health data) may be processed without consent (mother is abroad) in order to save the life of her child. Second, processing of ordinary personal data can be legitimate when this is in the interest of the data controller or a third party and when these interest are more important than those of the

data subject (Article 6.1(f) GDPR). Importantly, this ground legitimating data processing when in the interest of third parties does not apply with respect to the processing of sensitive data or the transfer of data. However, these articles do specify that personal data may be processed or transferred in the light of legal claims (Article 9.2(f) GDPR; Article 49.1(e) GDPR). This can be either claims by data subjects, by data controllers but potentially also claims by third parties (and hence in their interest).

Fourth and final, there is the situation in which the data processing is in the public interest. 'processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6.1(c) GDPR); 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (Article 6.1(e) GDPR). The data processing for the public interest should also have a basis in law (Article 6.3 GDPR – see also: Article 49.4 GDPR); the assumption is of course that if data processing is necessary for a task or obligation derived from a law with democratic legitimation, such data processing must be deemed in the public interest. With respect to processing sensitive data, most of the grounds contained in Article 9 relate to matters of public interest or national or EU law, such as 'field of employment and social security and social protection law' (Article 9.2(b) GDPR); 'substantial public interest, on the basis of Union or Member State law' (Article 9.2(g) GDPR); 'occupational medicine […] on the basis of Union or Member State law or pursuant to contract with a health professional' (Article 9.2(h) GDPR); 'necessary for reasons of public interest in the area of public health' (Article 9.2(i) GDPR); 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' (Article 9.2(j) GDPR). For the transfer of personal data, two grounds refer to public interests (Article 49.1(d) GDPR; Article 49.1(g) GDPR).

In other articles in the GDPR, reference is made to these principles, and especially consent and contract. For example, Article 7 lays down requirements for consent and specifies that in principle, revoking consent does not apply retroactively: 'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal' (Article 7.3 GDPR). Still, he does have the right to erase data when 'the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing' (Article 17.1.b). Also, the right to data portability applies when data are processed through automated means, the data subject has provided the data and 'the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)' (Article 20.1.a GDPR). In addition, the data subject should be informed 'whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data' (Article 13.1(e) GDPR). As a final example, Article 22 GDPR specifies that automatic decision making is not allowed, unless when this is based on explicit consent, is based on a law or is necessary for the contract between the data controller and the data subject; in ad-

dition, automatic decision-making based on sensitive data is not allowed, except when based on unambiguous consent or a substantial public interest.

The question is: what happens when interests clash?

When data processing is based on the public interest and the data subject feels it is not in his interest, he can claim that in his particular situation, his interests are higher or more relevant than the public interest (Article 21.1 GDPR). Consequently, the general presumption that certain data processing serves a public interest is not challenged (this is the democratic prerogative), although the data subject can obviously argue that data processing is not 'necessary' in order to achieve the public interest. The right to object shall apply when Article 6.1(e) GDPR is relied on; it is unsure whether this also holds true with respect to processing sensitive data and the transfer of data.

When data processing is based on the interest of the data controller or third party, the data subject can also argue that in his particular case, his interests are higher than those of the data controller (Article 21.1 GDPR) and he can argue that data processing is not 'necessary' for achieving the legitimate interests of the data controller or third party (interestingly, he cannot argue that the data controller misunderstands his own interests, though there are possibilities in the GDPR for the data controller to process data on behalf of the data subject without his direct or indirect consent). The right to object shall apply when Article 6.1(f) GDPR is relied on; it is unsure whether this also holds true with respect to processing sensitive data and the transfer of data. This also holds true with respect to the processing of sensitive data or the transfer of data in light of legal claims.

Finally, with respect to the processing of data in the interest of the data subject, there are two situations. First, the data subject has not consented directly or indirectly. What happens if personal data are processed because others believe that to be in the vital interest of the data subject, but the data subject disagrees (for example, the data subject wants to die, but doctors prevent that through emergency treatment) or when a contract has been concluded by others to serve his interests (Article 49.1c GDPR)? Second, with respect to indirect and direct consent, what happens if a person consents to something that is not in his best interest? Perhaps we would say that he must have not understood the information about the data processing, was misled or was simply unable to give legal consent (precisely because he did not protect his best interests).

Here it would be either way. Or, a formalistic approach will be taken; if the requirements of consent have been met (Article 4.11 GDPR; Article 7 GDPR; Article 8 GDPR), data processing will be valid, even if not in the interests of the data subject. Or, a material approach will be taken. Even if the formal requirements have been met, if the interests of the data subjects are not served by data processing, it will not be deemed not in compliance with the GDPR. And even if the formal requirements of consent have not been met, when the interests of the data subject have been served, this will be deemed GDPR-compliant.

If the former would be true, it would result in difficult situations, because the underlying presumption of consent is precisely that the data subject is capable of defending his own interests and should be facilitated in that choice by the data controller as far as possible. If the second were the case, why not just delete the notion of consent in the GDPR?

Deleting the notion of consent has a big advantage. Currently, many companies are mailing customers to give their (renewed) consent. Obviously, most people do not read the information that is provided to them; if they would, it would take them weeks to read all information and privacy policies. Removing consent from the GDPR would reduce the number of times consumers have to give consent significantly; right now, consent means virtually nothing because people get too many consent requests. In addition, it would put a stop to those practices that people consent to but are clearly not in their interest (though a hypothetical situation may be one where the data subject consents to processing his data by the controller, not in his own interests, but for altruistic reasons).

Companies could invoke two grounds: either data processing is necessary for the performance of the contract with the data subject (a data subject has signed an agreement to enter a social network; the social network can process personal data only in so far as this is necessary for the performance of that contract) – or the data processing is necessary for the legitimate interests of the data controller that are more important than those of the data subject. If they are not, then it seems only fair to stop the data processing.

I hope you enjoy reading this issue of the European Data Protection Law Review. It contains two opinions. The first is by Gus Hosein, the Executive Director of Privacy International. The second is by Artemi Rallo, the former Director of the Spanish Data Protection Agency.

We have three scientific articles. First, Catherine Jasserand has written about subsequent use of data for a law enforcement purpose. She questions the role of the principle of purpose limitation in a situation where personal data are collected under the GDPR and further processed under the regime of the Police Directive. Second, Lina Jasmontaite and colleagues have written about data protection by design and by default. They look at these principles both from a theoretical and a practical perspective. Third, Henry Pearce considers the right to data protection under EU law and examines a range conceptual and engages with questions regarding whether the right to data protection as contained in the EU Charter of Fundamental Rights confers on individuals proprietary or personal interests in their personal data.

As always, special mention should be made of the Reports section led by Mark Cole. Teresa Quintel has written on the opinions by the EDPS and WP29 concerning the Commission Proposals on the Interoperability of Databases. Juraj Sajfert has put together a report on the New Data Protection Regulation for EU Bodies. In the GDPR

series, Sharon McLaughlin has analysed the implementation of the GDPR in Ireland. Christina Etteldorf has written an interesting report on how in Germany, Data Protection Authorities Try to Fill the Gap between the GDPR and e-Privacy. And in the Practitioner's Corner, Jörg Ukrow has analysed the relationship between the EU GDPR and the Amended CoE Convention 108.

In the Case Notes section, there is a case note by Karolina Podstawa on the ECJ case of *Peter Nowak v Data Protection Commissioner* and another one by Sebastian Klein on the ECtHR case *Libert v France*. Finally, Claudia Quelle has reviewed a book by Radim Polčak and Dan Jerker B Svantesson entitled *Information Sovereignty,* and Lorenzo Dalla Corte has done a review of *Bulk Collection,* with Fred Cate and James Dempsey as book editors.

For those interested in contributing articles, reports, case notes or book reviews to the EDPL, please contact our executive editor Nelly Stratieva at <stratieva@lexxion.eu>. Below the deadlines for submitting contributions:

- Issue 3/2018: 15 July 2018 (special issue on health data; personal data processing in the medical sector)

- Issue 4/2018: 1 October 2018 (Young Scholars Award)

I hope you enjoy reading this edition of the European Data Protection Law Review!

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands