

Editorial

Suppose a person processes information about himself, for example online. He is the data subject, of course, but could he also be considered the data controller? The definition of the data controller does not exclude that the data controller can be the data subject himself, it merely states that the term controller refers to 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (Article 4.7 GDPR).

The Working Party 29 (WP29) has been rather vague about this possibility. For example, in its opinion on the concept of data controller, it stressed:

Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called 'household exception.'¹

It did hold that data subjects can be (joint) data controllers, but referred to 'uploading personal data also of third parties'. But what if a person only uploads personal data about himself on a social network – eg photos in which only that person is visible – wouldn't that person be qualified as a joint controller as well? And suppose a person uploaded personal data about himself on a website he himself built, shouldn't he be qualified as sole data controller?

If this is true, the GDPR would apply to such data processing, provided that the processing was done 'wholly or partly by automated means' (Article 2.1) and that, like the WP29 stressed, the household exemption does not apply. The household exemption states that the GDPR does not apply when data processing occurs 'by a natural person in the course of a purely personal or household activity' (Article 2.2c).

Where the boundary between purely personal or household activity on the one hand and professional or commercial activity on the other hand lies precisely is impossible to say (see also the rather vague Recital 18 of the GDPR). But the fact that the GDPR refers to 'purely' and the fact that the Court of Justice has, in the past, interpreted this exemption rather restrictively (see for example the *Ryneš* decision²), it would not be too difficult to imagine a situation in which the household exemption would not apply to the publishing of personal data by a data subject himself.

DOI: 10.21552/edpl/2018/3/3

1 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (16 February 2010) WP 169, 21.

2 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428.

Suppose, for example, that a famous celebrity keeps a blog about himself, to inform his fans and boost his public profile. He publishes about every aspect of his life – photos of the food he is eating, new work he is involved with, his music taste, his diagnoses of cancer, his chronic depression and his addiction to alcohol. Surely, such would not be a purely personal or household activity; it has the explicit aim of informing the public at large and his fans in particular. It has a potential commercial purpose and in any case a professional one.

If this hypothesis is true, it would mean that the data controller cum data subject must abide by the GDPR. Obviously, the rights of the data subject contained in Chapter III of the GDPR would be redundant: the data subject already has full information and can correct or delete the data whenever he likes. Most of the specific obligations for the data controller in Chapter IV will also not apply. There is the SME exception for keeping of records (Article 30.5) and it will be unlikely that the data controller cum data subject will need to implement a data protection impact assessment (Articles 35 and 36) or install a data protection officer (Articles 37, 38 and 39). Would the data controller need to make adequate technical and organisational security measures and adopt data protection by design or by default standards? Probably not, because the risks involved are low (though this might be different for specific situations) (Article 25 and 32). Also, the data controller does not need to inform himself of a data breach that has occurred (Article 34), though he might need to inform the Data Protection Authority (Article 33). Finally, it may not be deemed proportionate to demand of the data controller cum the data subject to implement a data protection policy (Article 24.2).

But other rules may have a significant impact, especially those in Chapter II of the GDPR. Although the data controller cum data subject would almost always have a legitimate ground for processing personal data and sensitive data, namely the data subject's consent (Articles 6, 7, 8 and 9 GDPR), the principles contained in Article 5 still apply. This would mean that the data controller cum data subject needs to respect those. This might have potentially interesting implications.

For example, could the data accuracy requirement entail that the person in question must tell the truth? After all, the data controller has the obligation to ensure that personal data that are being processed are accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

And what about the purpose specification principle, requiring that personal data may only be processed for concrete, specific and legitimate purposes. What would be the specific purpose at stake? Would boosting one's public profile suffice?

Most paternalistic potential lies in the data minimisation principle. What about, for example, the times that public persons make rather embarrassing statements or do rather awkward and startling revelations about themselves? 'I'm pregnant, but I slept with so many people that I don't know who the father is'; 'I drink myself to sleep with

a bottle of whiskey every night'; 'I have constant suicidal thoughts and tendencies', etc. Is that really necessary for the specific purpose at hand – boosting a person's public profile?

Could we say that this would not serve a legitimate purpose or that it is not necessary to process such personal data in order to reach the in itself legitimate purpose? If so, could we say that the data controller cum data subject is prohibited from publishing such information? And what if the person is not a public celebrity, but is just some lonely guy or girl hungry for attention? What would that mean for revealing sensitive data, such as health related information?

Turning to the matter of this edition, data protection in the medical sector is the main topic of Issue 3's article section, which was edited mainly by EDPL Board Member Alessandro Spina, who will introduce the five articles included in that section himself. To complement the five articles included in this edition, we have invited two internationally renowned professors to write a short opinion on the same topic. We are honoured by the contributions of Professors Giovanni Comandé and Gianluca Montanari Vergallo.

As always, special mention should be made of the reports section led by Mark Cole, which is one of the reasons why this journal continues to attract so many readers. There are reports on developments in Belgium, Germany, the Netherlands, Romania, the United Kingdom and one about the European Commission's E-Evidence proposal. The case notes section, led by Maja Brkan and Tijmen Wisman, includes three very strong case annotations written by Raphael Gellert, on door-to-door preaching, and Elena Kaiser, on the monitoring of employees, and by Marc Rotenberg and Natasha Babazadeh, on a new US Supreme Court decision. Finally, Alessandro Mantelero has managed three book reviews for his section, one written by himself on the new book by Mayer-Schönberger and Ramge, one written by Edoardo Celeste, about the book on governance of fundamental rights by Dawson, and the final one written by Silvia De Conca on the 2018 CPDP conference book.

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*