Final Draft 1.1 – This paper is accepted and will be published in Computer Law and Security Report 2016 - Please revert to CLSR once published

CiTiP Working Paper Series

Why research may no longer be the same: about the territorial scope of the Proposed Data Protection Regulation

Els J. Kindt

CiTiP Working Paper 26/2016

KU Leuven Centre for IT & IP Law

May 2016

This paper can be downloaded without charge from the Social Sciences Research Network electronic library (SSRN ID=1781425).

Why Research may no longer be the Same: about the Territorial scope of the New Data Protection Regulation

E. J. Kindt*

KU Leuven – Law Faculty – CiTiP– iMinds
Sint-Michielsstraat 6
B-3000 Leuven
els.kindt@law.kuleuven.be

*Post-doc legal researcher, KU Leuven – iMinds – CiTiP

Table of Contents

Abstract

In an innovative digital information society, research plays a key role. This research is no longer an individual and national activity, but is increasingly collaborative involving various resources, stakeholders and countries. For this purpose, research platforms are set up as they offer various advantages. In this article, we discuss examples of such research platforms and their benefits, including but not limited to the BEAT platform for biometric technology testing. After an analysis of the current and of the new territorial application rules under the data protection legislation, we investigate the consequences of these new rules for research and platforms in four particular situations. We warn and advise the regulator that research platforms and the use of other equipment for the collection and processing of personal data in the Union for research may escape from data protection legislation once the new data protection regulation applies. This is due to the revised territorial application rules in the new regulation. We therefore plead for more reflection and clear terminology and for keeping the criterion of the use of equipment for the territorial application of data protection legislation. Rejecting this criterion may result in considerable better (competitive) positions for non-Union companies and institutions collecting and using personal data collected in the Union for research as compared to Union research organisations.

Keywords

research – platforms - crowdsourcing - data protection – General Data Protection Regulation - territorial application – biometric testing – equipment – means - infrastructure – collection – testbed as a service - big data - transfer - co-controllers

Introduction

Research remains an essential pillar in making progress to the benefit of all in our digital society. Research activities, whether by commercial companies, governmental organisations or by academic institutions, continuously become more sophisticated and are organised in an increasingly international environment. New ways are invented to make data available and to make the collaboration between different stakeholders easy. One type of such innovative ways is the use of platforms. Such platforms which are developed and operated by one or more organizations, institutions or companies usually allow a high number of stakeholders to access and to participate in specific research. These platforms also allow in particular for the collection and storage of large amounts of personal data collected from volunteers or other individuals (data subjects) who may have agreed to provide their data for scientific research. These data collections often originate in the Union and can be from employees of companies, university staff but also from citizens and patients.

The EU Commission has acknowledged in its Digital Agenda in 2010 the increasingly important role that platforms play and will play, also for research.[1] Businesses have understood this as well and set already steps in this direction. Giants such as IBM and Johnson & Johnson, together with Medtronics and Apple announced their collaboration

[1] See EU Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe*, COM(2010)245 final, 19.5.2010, pp. 23-24. The Commission has also committed to assess the role of platforms in its Digital Single Market Strategy for Europe. See EU Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe*, COM(2015)192 final, 6.5.2015, pp. 11-12, and the public consultation on platforms which ran from September 2015 until early January 2016.

in April 2015 for a so-called 'Watson Health unit'.[2] Partners are intending to use health information gathered by millions of Apple devices and to aggregate health information from a large number of devices and providers in the cloud for research purposes. An important aspect thereof is the use of advanced data analytics and predictive analytics by a new unit with headquarters in Boston.[3] For this type of research, massive amounts of data are necessary.

Various other platforms on national and international level in other domains are also being developed or operated for a variety of purposes. There are examples of platforms needed for the development of 'smart cities' and the Internet of Things, platforms dedicated to specific purposes such as crowdfunding and community building[4], or for education, where schools team up with the publishing sector[5], or more generally, platforms for staying 'motivated and improve your health by tracking your activity, exercise, food, weight and sleep'.[6]

Platforms are furthermore developed in European projects, which are after the project made available according to the exploitation plan, to a larger user group to stimulate research or to allow comparison of for example testing results of algorithms. Such platforms are often coded in open source software allowing future acquireres to improve or to customize the platform. This open source software approach implies that these platforms will under an appropriate license be 'floating' around in the research communities, whether inside the Union or outside, in order to ensure a wide take-up and for advancing knowledge and research in particular domains in the interest of science and public interest. An example is the BEAT platform. The BEAT platform has been developed to meet the need for more biometric technology testing.[7] Other examples of research platforms used in European projects, include the platform IoT Lab and Fed4Fire, the latter providing a platform and aimed at federating heterogeneous testbed infrastructures.[8]

This article discusses some results of the legal research in the context of the BEAT project.[9] After a short description of the importance of research platforms, we stress the need to carefully assesses the modifications to the European data protection legislation as they impact research and have as a consequence that the collection of personal data in the Union and the use of such data collections on platforms for research by non-Union controllers escape from such legislation. We hereby look at some newly suggested rules for the use of personal data for research and at the territorial scope in the New Regulation, of which the proposal was initiated by the EU Commission on 25 January

[2] See X., *Johnson & Johnson and IBM Announce Plans to Collaborate on Advanced Solutions Designed to Transform Healthcare Delivery*, 14.4.2015, available at https://www-03.ibm.com/press/us/en/pressrelease/46582.wss

[3] IBM bought for this purpose two health technology firms, Explorys and Phytel, specialized in health data analytics. See B. Rigby, *IBM launches new health unit, teams up with Apple, J&J, Medtronic*, 13.4.2015, in Reuters, available at http://www.reuters.com/article/2015/04/13/us-ibm-healthcare-idUSKBN0N427220150413 See also X., *ODH, Inc. and IBM Watson Health Introduce Mentrics™, a Population Health Management Platform to Transform Behavioral Healthcare*, 20.4.2016, available at *https://www-03.ibm.com/press/us/en/pressrelease/49564.wss* : '(...) the system will *gather and aggregate health data*, including behavioral and physical medical services and prescription claims, *from fragmented sources* into one easy-to-use *platform* that can deliver *comprehensive and predictive insights* (…)' (italics added).

[4] See, e.g., the French Ulule platform, embraced by the banking institution BNP Paribas. See http://www.wave-innovation.com/en/ulule.html

[5] See e.g., in Belgium, Bingel, a platform developed by publishers for primary school students. See http://www.bingelsite.be/nl

[6] See Fitbit official site for activity tracking at https://www.fitbit.com/

[7] The BEAT platform is developed under the grant agreement 284989 of the 7th Framework Programme. About the BEAT project, see https://www.beat-eu.org/

[8] See IoTLab. Crowsource The Future, available at http://www.iotlab.eu/ and Fed4Fire. Federation for Future Internet Research and Experiments, available at http://www.fed4fire.eu/testbeds/

[9] See also the public deliverables D 9.2 entitled 'Guidelines for Privacy and Data Protection' and D 9.3 entitled 'Analysis of current practices of use of biometric data for research purposes', both available on the website of the BEAT project.

2012. The European Parliament adopted its position on an amended text version in first reading on 12 March 2014 and an agreement about the overall compromise text for the New Regulation was reached by the representatives of the European Parliament and the Presidency on 15 December 2015 following ten trialogues between the EU Commission, the EU Parliament and the EU Council. On 8 April 2016 the final text was adopted by the Council and on 14 April 2016 by the EU Parliament, and was published in the Official Journal on 4 May 2016 ('New Regulation' or 'GDPR')[10]. The GDPR replacing Directive 95/46/EC will be effective two years and twenty days after this date of publication.

We argue in this article that the new rules on the territorial scope impact the collection for research purposes of personal data by non-Union controllers through means or equipment used or operated on Union territory. Think for example about the wearables, smart watches or apps installed on smart phones and held by data subjects in the Union for the collection of data concerning health and which are used for further research by companies outside the Union. We warn that platforms and more generally any equipment located and used in the Union for the collection and the processing of personal data in the Union (other than for transit), but controlled from outside, may under the new data protection legislation escape from data protection regulation as developed in the Union, due to the revised territorial application rules in the New Regulation.

We use the term 'research' as a general term not bound to any particular definition. It includes use of personal data for archiving purposes (in the public interest), scientific and historical research and use for statistical purposes in general, whether by a not for profit organization, a governmental institution or commercial company.[11] Further, please note that the examples of data collection and research collaborations mentioned in this article are just illustrations of the increased importance of data collection and shared use for research purposes and which may thereafter result in any service or product development. The legal analysis hereunder does not specifically relate to any of these examples.

1 Importance of personal data collection and of research platforms for advances in scientific research

1.1. The importance of personal data collection for research

It is common ground that increased storage and processing capacities facilitate massive personal data processing activities. Rather new is the expansion of infrastructures that allow these activities around the globe. These structures provide for massive collections of personal data, sometimes also crowdsourcing, for example as collected by smart devices, and provide for storage, for example in warehouses often 'in the cloud', and the shared processing, all on so-called platforms. In the near past, the data collected has been

[10] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, pp. 1-88, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL ('New Regulation' or 'GDPR').

[11] One could debate as to whether the use of personal data collected by a company 'to improve their services and develop new services' is research or not. Research activities however are not limited to not for profit or governmental organizations only. See also the New Regulation which describes scientific research purposes in a broad way: '(…) For the purposes of this Regulation, processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research, privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. (…)'. Recital 159 GDPR.

used to make profits by selling.[12] But with new data analytic methods and progress in predictive analysis, the data become increasingly important for further use for research as well. For this new type of data use and research, mass collection of personal data is essential.[13]

The data is hereby increasingly collected from data subjects by infrastructures held or worn by these data subjects. Think of for example smart wristbands. While the data subjects will expect in some cases to receive particular services in return for uploading their personal (health) data, such as personal monitoring of sleep patterns and coaching for changing behaviour, this is not always the case. The message is passed on that mass collection of data can be useful to advance medical research, for example in the detection or prediction of cancer, or in the common interest. Learning that massive data sharing may help other people, individuals are often agreeing or even eager to share their data gratuitously. This new trend is referred to as data philantropy, or as the vice-president of the new IBM Watson health unit described it: "The generation who buy Apple Watches are interested in data philanthropy," he said. "Many of them have been touched by relatives or parents struck down by disease. Why wouldn't they help researchers figure out what's going on?"[14] Others refer in this context to crowdsourcing, crowddriven research and participatory action research.

1.2. The importance of research platforms

But 'wearables' are not the only new devices for data collection and processing. Another (additional) type of infrastructure that is increasingly used and available, also for innovation and research purposes, are platforms. While it is difficult to define 'platform', one could describe it generally as a common infrastructure where different users can directly or indirectly easily upload, store, access, process and share information located with the platform or elsewhere, and interact with one another. 'Platforms' exists in a large variety of industries. Social network services operate an online communication platform, cloud providers provide development and test platforms, while service specific applications also increasingly move towards platforms. But especially in high-tech businesses driven by information technology, platforms become indispensable whereby all the firms and partners involved participate in what is called a platform-based "ecosystem" innovation.[15] They often represent a researchers' community based approach and allow researchers to share data and to test their designs. Gawer and Cusumano have described and analyzed this phenomenon of 'platforms' very well[16] and we refer to their well documented work and literature study to gain a better understanding of the concept. It should become clear that platforms are hence very important for innoviation, research and development. Innovation platforms serve, as

[12] Major companies, such as IBM, Quest Diagnostics, … for example, derived significant revenue and immedaite commecial gain by selling sensitive personal data, such as personal health data, including to governments. See D. Peel, 'IMS Health Files for IPO - Is It Legal ?', on Patientprivacyrights, 5.1.2014, available at https://patientprivacyrights.org/2014/01/ims-health-files-ipo-legal/

[13] Crowdsourcing, whether limited to individuals who have previously registered (private crowdsourcing) or open to a broad group (public crowdsourcing), and (passive or participatory) crowdsensing play hereby an important role. See also J. Howe, *Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business*, N.Y., N.Y., Crown, 2008, 320 p.

[14] D. Crow, 'IBM strikes digital health deal with Apple, Medtronic and J&J', in FT.com, 13.4.2015, available at http://www.ft.com/intl/cms/s/0/c6ac2792-e179-11e4-9b30-00144feab7de.html#axzz3p0IFyR8o

[15] Gawer, A. and Cusumano, M., *Industry Platforms and Ecosystem Innovation*, 2012, p. 1, available at file:///C:/Users/Gebruiker/Downloads/98590.pdf ('Gawer and Cusumano, Industry platforms, 2012'). See also A. Gawer (ed.), *Platforms, Markets and Innovation*, Elgar, 2011, 396 p.

[16] E. g., in their paper, they define internal (company or product) platforms 'as a set of assets organized in a common structure from which a company can efficiently develop and produce a stream of derivative products (Meyer and Lehnerd, 1997; Muffato and Roveda, 2002)', while they define external (industry) platforms as 'products, services or technologies that are similar to the former but provide the foundation upon which outside firms (organized as a 'business ecosystem') can develop their own complementary products, technologies, or services (Gawer and Cusumano, 2002; Gawer, 2009a).' Cited fromGawer and Cusumano, Industry platforms, 2012, p. 2.

Gawer describes, as a technological basis on top of which other firms develop complementary innovation. The use of these platforms and the supply of personal data by data subjects is crucial to these companies, so various types of products, services or games connected with these platforms are developed. The boss of Amazon.com described it during a life blog about Kindle and the Kindle books store in 2012 as follows: 'We want to make money when people use our devices, not when they buy our devices'.[17]

Platforms for data collection and processing also are part of the new datafication trend. The term datafication refers to 'taking information about all things under the sun' and 'transforming it into a data format to make it quantified'.[18] Multiple data collections gathered from different players, sometimes even of competitors in traditional businesses[19], are hereby stored on the platform and made available for, for example deep learning and big data research, while pursuing common interests. Such platforms are hence used as testbeds to collect and to upload the personal data collected from data subjects and to share such data with collaboration partners, whether they are established inside or outside the Union.

Platforms can also be used to store already collected and existing databases. Platforms offer for example the advantage of sharing of testing results on (same) data with a larger community rather than keeping results in a small circle of experts.[20] Platforms hereby allow other parties to verify claimed testing results against the same set of data made available with the platform. In other words, the platform enables repitition of testing results obtained with for example a particular algorithm and to attest the results against a same set of data. An advantage of platforms is hence that the researchers can dispose over (large) collections of personal data stored with the platform without the need to collect or to (download and) install themselves various testing databases. Another advantage of platforms is that the researchers can perform research and testing without the need to (download and) install various software programmes needed for and enabling the testing. Other terminology used in this context includes testbeds as a service (TBaaS).

2 New rules on research in the GDPR

Under the present general data protection Directive 95/46/EC[21], research is only in a fragmented way mentioned in the Directive. First, the requirement that personal data cannot be re-used, *i.e.* further used for purposes in a way incompatible with the previously specified, explicit and legitimate purposes, is loosened for 'further processing of data for historical, statistical or scientific purposes' upon the condition that Member States provide 'appropriate safeguards'.[22] In other words, personal data processing for research purposes can disregard the initial collection and processing purpose(s) as long

[17] See J. Bezos, founder and CEO of Amazon.com, 'Life from Amazon's Kindle Event: New Kindles, Kindle Fire HD unveiled', 6.9.2012, Wired.com, available at http://www.wired.com/2012/09/amazon-kindle-event-live-blog/

[18] K. Cukier and V. Mayer-Schonberger, *Big Data: A Revolution that will transform how we live, work and think'*, 2013, p. 15.

[19] See also Gawer and Cusumano, Industry platforms, 2012, p. 7 : 'In parallel with the strategy literature, some researchers in industrial organization economics have begun using the term platform to denote markets with two or more sides, and potentially with network effects that cross different sides. Such a "multi-sided market" provides goods or services to several distinct groups of customers, all of whom need each other in some way and rely on the platform to mediate their transactions (Evans, 2003; Rochet and Tirole, 2003 and 2006).'

[20] Platforms such as BEAT allow and encourage to share findings in international research activities, such as in the field of biometric technologies by means of the platform. The platforms is then used, such as in the example of BEAT, for testing algorithms or organizing competions.

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, pp. 31-50 ('Directive 95/46/EC').

[22] Art. 6.1(b) Directive 95/46/EC and Recital 29.

as national laws providing for safeguards for using personal data for research are respected. Such national laws would for example impose encoding data or even anonymisation before using the data. Personal data should also not be kept in a form which permits identification for longer than necessary for its processing purposes. In other words, personal data should be anonymized as soon as identification is no longer required for the original or secondary processing purposes (other than research). Member States however may again deviate from this rule for data used for research provided they lay down 'appropriate safeguards'.[23] There is also an exemption from the information obligation, for processing for statistical purposes or for purposes of historical or scientific research, if the (later) recording or disclosure is expressly laid down by law or if giving information proves impossible or would involve disproportionate effort, provided the Member States provide 'appropriate safeguards', and from the right to access, again subject to national 'adequate legal safeguards'.[24] Finally, exemptions on the prohibition to process sensitive data may also be authorized on grounds of 'sustantial public interest' such as 'scientific research and government statistics', subject to 'specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals'.[25]

It is clear from these provisions that the use of personal data for research is currently almost a purely 'national matter' of 'appropriate safeguards', and not at all harmonized across the Member States. Research organizations and companies in the Union have to apply these specific and very national rules for their data use for research. Compliance with these varying rules is very demanding for research organizations established in the Union, especially where for example pseudonymisation or anonymisation is imposed, and this to protect the fundamental rights and the privacy of individuals.[26]

In the new General Data Protection Regulation ('GDPR', Article 5.1(b) states that '(…) further processing (…) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'. A distinct provision Article 89 GDPR is now dedicated to data processing for research purposes. Article 89 GDPR has however been modified considerably during the first reading of the European parliament and then by the Council. [27] In the final text, it is stated that Union or Member State law may provide for derogations for various GDPR articles, in particular for the right to access and the right to rectification, the right to restriction of processing, for the notification obligation of the controller regarding rectification or restriction and to the right of the data subject to data portability (both only for the processing for archiving purposes in the public interest) and the right to object, subject to the appropriate safeguards and 'in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of these purposes'. Union or Member State law hereby retains less possibilities to derogate than in the former draft text as amended by the Council.[28] At the same time, article 89(1) GDPR imposes that appropriate safeguards for

[23] Art. 6. 1(e) Directive 95/46/EC.
[24] See Art. 11.2 Directive 95/46/EC and Recital 40 and Art. 13.2 of Directive 95/46/EC.
[25] Art. 8.4 Directive 95/46/EC and Recital 34.
[26] See e.g., an obligation imposed by law to anonymize the data or, if the research could not be conducted with anonymized data, to encode the data: (Belgian) Royal Decree of 2001 for the execution of the Act of 8 December 1992 for the protection of the personal sphere with regard to the processing of personal data, 13.02.2001, *B.S.* 13.3.2001.
[27] See and compare with the initial text in Art. 83: European Commission, Proposal for General Data Protection Regulation COM(2012) 11 final. For the amendements by the European parliament and the Council (status as of 15 July 2015), and the suggestions of the EDPS, see EDPS, Annex to Opinion 3/2015. Comparative table of the GDPR texts with EDPS proposals, available at **Error! Hyperlink reference not valid.** For the final text (with renumbering), see footnote 10 ('New Regulation' or 'GDPR').
[28] In this text version, derogations were also possible for the processing for archiving purposes, for the data protection by design and default obligations, the data breach provisions, the impact assessment obligations and the investigative powers of the supervisory authorities, and for all research, for the information obligation, all were necessary for the fulfilment of the particular purposes. See text of art. 83.1 GDPR and of art. 83.2 GDPR, as amended by the Council (for this text, see footnote 27 *above).*

the rights and freedoms of the data subject shall be respected, and that these shall 'ensure that technical and organisational protection measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation, provided that those purposes can be fulfilled in this manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permit the identification of data subjects, those purposes shall be fulfilled in that manner'.[29] The measures of pseudonyimisation and anonimisation for personal data for the use for research purposes is hereby clearly stated. It should hence become clear that the use of personal data for research purposes requires compliance with specific, stringent and often time consuming obligations.

The need of implementation of the Directive 95/46/EC by the respective Member States resulting in a 'stack' of applicable national laws for international activities has been considered one of the main weak points of Directive 95/46/EC. This was often critized, not at least because the national laws had implemented the Directive 95/46/EC in different ways.[30] In view of the propositions of the Council for derogations to the fore-mentioned article as described, one wondered whether the Regulation would offer much relief in this respect for data processing for research since Union but als Member States' law could impose and require respect of additional safeguards. In the final text, the manoevre space for additional Union or Member State law is reduced, but remains in our view considerable. It is clear that full harmonization of the data protection rules – one of the major goals of the reform – will not be achieved for research and data processing activities in the Union. This will result in even more difficulties for research organisations established in the Union to comply.

At the same time, the new rules on the territorial scope of the data protection legislation, seem to forget non-Union research organisations established outside the Union using personal data collected from data subjects in the Union for research. This hole in the territorial scope results in a more advantageous position for such organisations collecting or using data of data subjects in the Union for research purposes. We explain this further.

3 Current territorial scope under the Directive 95/46/EC

After a long period of raising limited concern and passing largely unnoticed, the provisions on the territorial scope of the data protection legislation have gained recently more attention. Disputes with some social network applications[31] but also particular decisions rendered by the European Court of Justice ('ECJ') triggered this, in particular since the *Google Spain* case of May 2014. In *Google Spain*, the ECJ declared the European data protection principles applicable to activities of Google Inc. established overseas.[32]

The current territorial application rules are laid down in Article 4 of the Directive 95/46EC. Article 4(1)(a) explaines that various (and hence more than one) national data protection legislations of different Member States will apply if the controller has establishments on different territories of Member States ànd processes personal data in the context of the activities of each of these different establishments. The place of the establishment ànd the activity of that establishment is hence determining the applicable

[29] See Art. 89.1 GDPR.
[30] For an overview of the implementation of the Directive in the (then) 27 Member States, see European Commission, *Status of implementation of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data*. For the consultation input, see EU Commission, 31.12.2009, available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm and for the input of stakeholders on the consultation (COM(2010)609, see EU Commission, 15.01.2011, available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm
[31] See, e.g., Facebook Inc, which holds that national Member States laws other than from Ireland, place of its main establishment in the Union, are not applicable.
[32] See further *below*.

national data protection legislation. In traditional European private international law theory for contracts and torts, the applicable law is determined by a 'closest connection test'[33], whereby the characteristic performance doctrine ('where does the most characteristic activity takes place') is applied. For data protection legislation, the processing of personal data is the most characteristic element and the closest connection the place where this processing takes place, both criteria chosen as linking factors to determine the national data protection rules of that Member State to be applied in case the controller is established in the Union.[34]

In case the controller responsible for processing the personal data would not be established in the Union, the national data protection legislation of the location of equipment used by that controller to process personal data would apply. If the controller is not established in the Union, Article 4(1)(c) of the Directive 95/46/EC states that the use of equipment[35] or means[36] (other than for transit), automated or otherwise, situated on the territory of a Member State, would determine the national applicable law.[37] The notion of equipment is broadly interpreted (see also *below*). As stated, article 4(1)(c) Directive 95/46/EC gained more importance over the years with new Union wide used applications and new types of data processing fed by users in the Web version 2.0, but controlled by companies outside the EU, such as search enginges and social networks.

Over time and in general, however, European private international law has been taking over more elements of common law in its harmonization policy and codifications aimed at 'conflicts resolution', with a stronger emphasis on the citizen. Such common law would for example stress the appropriateness (common law) with predictability (which is a more continental Europe concern) in a growing more complex world.[38] This would lead to a correction mechanism to the characteristic performance doctrine: other laws could be taken into account if there is (manifestly) a closer connection.[39] For the GDPR, the concern that data subjects in the Union needed better protection by European data protection legislation if their data was used by companies not established on Union territory prevailed, and resulted in a specific provision in the GDPR that European data protection legislation applies if they are targeted, or, in other words, if their personal data are processed for the 'offering of goods or services' to them and in case of their 'monitoring'. Recital 23, as amended, is quite clear in this respect. The tendency to correct the characteristic performance test by appropriateness hence seems to have played an important role in taking a 'service oriented approach' for the territorial application of the new data protection rules in the new Regulation by taking the 'targeting' into account and introducing the new criteria of 'offering of goods or services' to data subjects in the Union and the 'monitoring of their behaviour'.[40] In the

[33] This is also applied by the Rome I Regulation 593/2008 for civil and commercial contractual matters and in the Rome II Regulation 864/2007 on the law applicable to non-contractual obligations.

[34] See also the Data Protection Authorities in Article 29 Working Party, *Opinion 8/2010 on applicable law*, 16.12.2010, WP 179, pp. 10-17 ('Art. 29 WG, Opinion on Applicable law, 2010').

[35] This is the wording used in the English version of the Directive 95/46/EC.

[36] 'Means'is the wording used in most other language versions of the Directive 95/46/EC. See about the meaning and last minute changes during the preparation of the Directive 95/46/EC and the implementation in national laws, D. Korff, *EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws*, Cambridge, 2002, pp. 47-48 (Korff, Study on Implementation, 2002'), and L. Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? ', *IDPL* 2011, pp. 33-34 ('Moerel, Long Arm, 2011').

[37] Some mention that this Art. 4. 1(c) was mainly aimed at those situations where a controller would try to escape from application of the law by establishing itself outside the Union. Consequently, by adopting a 'target' approach in Art. 3.2 GDPR, this Art. 4. 1(c) would no longer be required. See also Art. 29 WG, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*, 30.5.2002, WP 56, p. 5 ('Art. 29 WG, Working Document non-EU based websites, 2002'). We do not believe however that this Article is only aimed against this type of practice. Offering protection on Union territory remains equally important (see also *below*).

[38] See also G. Van Calster, *European Private International Law*, Oxford, Hart, 2013, pp. 136-137.

[39] See also e.g., Rome Regulation I, Art. 4(3) and Art. 4(4) and Rome Regulation II, Art. 10.4.

[40] See also the suggestion made by the Data Protection Authorities in 2010: Art. 29 WG, Opinion on Applicable law, 2010, p. 31. Suggesting 'targeting' or 'directed activity' as also mentioned in the Rome Regulation I for consumer contracts, as new criterion; see also Moerel, Long Arm, 2011, p. 45.

text amended by the Council and the compromise text, to 'monitoring' was added 'as far as their behaviour takes place within the European Union'. The EU Commission also hopes to reach more singularity of jurisdiction by harmonizing applicable law by the New Regulation.[41]

We however warn for dropping and replacing the criterion of the use of (processing) equipment[42] in the GDPR in case the controller is not establisched in the Union by the new and sole criterion of offering goods or services to the data subjects or their monitoring, for the reasons we will explain below.

As already said, the first major test of the territorial scope of the EU data protection legislation came with the European Court of Justice (ECJ) case in *Google Spain.*[43] In that case, a data subject in the main proceedings filed a complaint to the national Data Protection Authority ('DPA') and asked from Google Spain and Google Inc. to remove particular pages from the Google search results. In the request for a preliminary ruling to the ECJ by the DPA opposed to Google in national proceedings, the ECJ interpreted in its decision the connecting factor and hence the processing 'in the context of the activities of an establishment of the controller on the territory' deliberately in a broad sense.[44] In the case, there was an establishment of Google Inc. in Spain which activities were considered by the Court to be 'inextricably linked' since 'the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable'. The Court also stated that 'that engine is, at the same time, the means enabling those activities to be performed'.[45]

The appropriateness of extending the territorial application to Google's establishment in Spain and hence of declaring European data protection legislation principles applicable was defended by the Court by stating that 'it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental righs and freedoms of natural persons which the directive seeks to ensure (…)'.[46] In other words, the Court in our view already took – based on the existing

[41] Jurisdiction (forum – competent courts – also 'conflict of laws' *stricto sensu* under common law where courts have to review other than their own domestic law) is obviously a different matter and to be distinguished from the issue of applicable law. Desirable but often non-alignment of both applicable law and jurisdiction lead to particular issues for data protection law. We do not further discuss the jurisdiction aspects of the applicable law in this contribution.

[42] The characteristic performance test as in the use of (processing) equipment physically connects the protection offered by the data protection legislation to the place where data are actually processed, in particularly collected and stored. We will argue that in addition, a reference to the processing of personal data of data subjects in the Union, should be added in order to avoid a too broad application.

[43] ECJ, C-131/12, *Google Spain SL, Google Inc. v. AEPD, Gonzalez,* 13.5.2014, ('Google Spain 2014') available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

[44] See Google Spain 2014, § 53. See also in a similar broad way to render Belgian law applicable to the placement of datr cookies on computers of non-Facebook users in Belgium, Vz. Rb. Eerste Aanleg, *Debeuckelaere v. Facebook Inc., BVBA Facebook Belgium and Facebook Ireland Limited*, 9.11.2015. We refer also to earlier drafts of the Directive 95/46/EC in which 'established' in Article 4(1) (a) was later modified to the 'processing in the context of activities of an establishment' of the controller. This modification however was not made (and may probably by accident have been ommitted) in (the present) Article 4(1)(c) during the same preparatory work. See Commission, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM(92) 422 final, *OJ* C 311, 27.11.1992, pp. 30-61.

[45] Google Spain, § 56. The ECJ hence did not rely on Article 4(1) (c), but on Article 4(1)(a) to declare EU data protection law applicable to Google Inc. established in the U.S. This was in our view somewhat surprising. First, because this Article 4(1) was aimed at deciding national applicable law(s) when the controller is (clearly) established in the Union. Second, Article 4(1)(c) of the current Directive 95/46/EC could have been relied upon as well by the ECJ, e.g., based on the cookies used by the engine and installed on equipment and the existing 'cookies equipment theory' to declare European data protection law applicable as well. For this theory, see *below*.

[46] Google Spain, § 58.

territorial scope rules - the target and the direction of offering of services towards Union persons residing in the Union in an indirect manner into account in its judgement.[47]

The ECJ continues in the same manner in *Weltimmo*.[48] In this case, the Court interpreted 'establishment' quite broad as 'it cannot be interpreted restrictively' 'in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules'.[49] It answered in a request for preliminary ruling that 'the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement' 'if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for the provision of the specific services concerned in the Member State in question'.[50] The Court further took various other elements into account, such as the (Hungarian) language used, the fact that the website dealt with properties located in Hungary and the opening of a bank account and the use of a letter box in Hungary, capable – according to the Court – to be an 'establishment' within the meaning of Article 4(1)(a) of the Directive 95/46/EC. In our view, the target and the direction of the offering of services towards Union persons residing in the Union was again clearly taken into account in its judgement, such in conformity with consumer protection law and the 'directed activity' approach as also mentioned in the Rome Regulation I for determining applicable law for consumer contracts, even before the adoption of the modifications in the GDPR. The Court hereby seems to place the territorial scope provisions of the Directive 95/46/EC in a larger context of Union law as a whole. We should further note that particular physical elements located in the territory of Hungary were taken into account as well for discerning an establishment as representation of the controller.

While the Court did not rely on the 'equipment' criterion, although mentioning if for the interpretation of 'establishment', one could argue that such criterion of 'equipment', in view of this decision, would no longer be required. It should be reminded though that this case involved questions relating to applicable law in a Union context with entities established in the Union, where the use of 'equipment' was less important. This is different if the controller is not established in the Union. Taking 'equipment' elements into account under the 'establishment' criterion could create therefore in our view confusion.

This interpretation of the ECJ in *Google Spain* and later decisions as mentioned does in our view not affect the need to carefully reflect on the applicable law to the collection of personal data by and the use of research platforms in the Union controlled by organizations established outside EU without any establishment in the Union. When controlling and using equipment (*i.e.* the platform) located in the Union, the present Article 4(1)(c) of the current Directive 95/46/EC extends data protection (legislation) based on the 'use of equipment' criterion to platforms where data subjects' (whether Union nationals or not) data are used and processed for research processes even if such data processing on the platform is controlled from outside the Union. Such use for research is in many cases directed to any data subjects from whom the data are collected for offering goods or services nor to monitor their behaviour.

---

[47] See Google Spain, § 58: 'It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, (…) when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to *promote and sell advertising space offered by that engine* and which *orientates its activity towards the inhabitants of that Member State*.' (emphasis added). For more analysis of this important case, see e.g., B. Van Alsenoy, A. Kuczerawy, and J. Ausloos, 'Search enginges after *Google Spain*: internet@liberty or privacy@peril?', ICRI Working Paper Series, 73 p.; H. Kranenborg, 'Google and the Right to Be Forgotten', Case Note, *EDPL* 1, 2015 pp. 70-79; B. Van Alsenoy and M. Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'', *IDPL* 2015, pp. 105-120.

[48] ECJ, C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabads ág Hatóság,* 1.10.2015 ('Weltimmo').

[49] Weltimmo, § 30.

[50] *Ibidem.*

4 New rules on the territorial scope in the GDPR

4.1 The new Article 3 GDPR on the territorial scope

The New Regulation changed radicaly the rules on the territorial scope, especially for the case where controllers are *not* established in the Union. One reason is without doubt the fact that processing operations by companies outside the Union target increasingly data subjects (e.g. when using various types of (mobile) apps) for advertising and selling products and services. Another reason of the changes could be reduced to the given that data processing activities are no longer bound to fix locations, but spread out 'in the cloud', whereby it is more difficult to know in which country the processing activities takes place.

For these reasons, the Commision, the European Parlement and the Council opted in the GDPR to focus - besides the location of controllers and processors and their data processing activities in the Union - on the location and the protection of data subjects in the Union. This is in line with a broader attention to consumer protection and with the political aim of offering more data protection to data subjects in the Union and rendering data protection more effective.

Article 3.1 GDPR maintains the principle that the data protection legislation applies if the data are processed in the context of activities of an establishement of a controller on Union territory, while adding after controller '*or a processor'*.

Article 3.2 GDPR states that – if the controller or processor[51] is not established[52] in the Union - when personal data of data subjects in the Union are processed ànd when the processing is related to the offering of goods or services to data subjects in the Union or the monitoring of behaviour of these individuals in the Union (for example, on websites), the GDPR will apply. Recitals 22, 23 and 24 further explain the intention of the legislator. Recital 23 GDPR states it as follows: '(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union'.[53]

[51] This was amendment 97 by the Parliament in Art. 3.2 GDPR.

[52] Note that the text of the GDPR maintains different terminology for referring to 'establishment': in Art. 3.1 'in the context of the activities of an establishment' and in Art. 3.2 'not established in the Union' which is similar as in the Directive 95/46/EC and which has already been discussed and interpreted in literature in various ways. Please also note that in this case of Art. 3.2 GDPR, this would include the obligation to appoint a representative in the Union (see Art. 27 GDPR).

[53] For the EP's compromise suggestion for (the then numbered) recital 20, see Council of the European Union, Interinstitutional File 2012/0011 (COD), 10366/15, 2.7.2015, pp. 7-8, available at http://data.consilium.europa.eu/doc/document/ST-10366-2015-INIT/en/pdf

With regarding to the monitoring, this is further explained in Recital 24 GDPR as follows :'(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes places within the European Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes'.[54] This Recital 24 seems to view tracking as tracking on the Internet. Looking further at the EP's proposal, we note that the EP's proposal included processors and made also reference to the 'collection of data' 'including from public registers and announcements in the Union that are accessible from outside of the Union' besides tracking. The EP's proposal for this Recital 24 hence seemed to interprete Article 3.2 GDPR broader. The explicit reference to collection was however not retained in the final text of this recital.

The location of the data subjects (whether domiciled or residing or travelling, whatever their nationality) hereby becomes the criterion. This is in our view a good evolution. The aim should indeed be the protection of the citizens and residents and all other natural persons in the Union by a high level of data protection.[55] At the same time, however, the scope of the protection offered to the citizens and residents and other natural persons in the Union is again narrowed by adding a material element that the data processing should relate to the offering of goods or services (even if no payment is required) or is related to the monitoring of behaviour. It is unclear why this material element should narrow the scope of the territorial criterion. Is all other personal data collection and processing of persons in the Union for other purposes not in need of protection ? At the same time, the GDPR does no longer retain the use of equipment physically located in the Union as a connecting factor. We did not find much indications that this was well thought about or explanations why this criterion was dropped all together.

The new Article 3 GDPR poses problems. We discuss them hereunder, while focusing on data processing for research purposes.

4.2 The addition of 'or a processor' in Article 3.1 GDPR

Article 3.1 GDPR states that the 'Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union (…)'.[56] In the compromise and final text, it was added 'regardless of whether the

[54] The EP's compromise suggestion was as follows :'(21) The processing of personal data of data subjects residing in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of such data subjects. In order to determine whether a processing activity can be considered to monitor data subjects, it should be ascertained whether individuals are tracked regardless of the origins of the data, or if other data about them are collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent use of data processing techniques which consist of profiling 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. [The Presidency suggests to maintain the Council General Approach, subject to redrafting]'. The Presidency suggested to maintain the Council General Approach, subject to redrafting but also considered accepting this EP compromise proposal for (the then numbered) recital 21, which is 'acceptable in principle subject to redrafting'. See Council of the European Union, Interinstitutional File 2012/0011 (COD), 10366/15, 2.7.2015, p. 1 and pp. 9-10, available at http://data.consilium.europa.eu/doc/document/ST-10366-2015-INIT/en/pdf

[55] See also the ECJ in Google Spain 2014 and its references in § 58.

[56] See also Council of the European Union, Interinstitutional File 2012/0011 (COD), 10366/15, 2.7.2015. The Presidency suggests to maintain the Council General Approach, while taking into account recital 19.

processing takes place in the Union or not'. First of all, the addition in Article 3.1 GDPR 'or a processor' is new and its full meaning confusing. While the processor is getting a more responsible role in the GDPR[57], does Article 3.1 implies that *only the provisions applicable to processors* will apply if the processor is established in the Union (e.g., the provisions on the security (technical and organizational means) of the processing) ? Or does the new *Regulation applies as a whole* (to the data processing activities of the controller) as soon as a processor established in the Union is appointed by this controller and processes any personal data on its behalf? This is crucial. The first solution would seem logical. J. Albrecht commented in July 2015 that the three parties 'have fixed the market location principle' 'so that there is no misunderstanding that realy everyone who acts on the European market has to follow the new rules on data protection enshrined in this Regulation and that this will be not only applicable to data controllers but also to data processors'.[58] From the addition 'or a processor' in the GDPR, it entails more clearly that the processor also has to live up to the national data protection rules of the place where the processor is located. Until now, it is not always clear which national law is to be applied to the assessment of the security obligations.[59] At the same time, it is not expressly stated in Article 3.1 GDPR that the establishment of the processor in the Union would render the Regulation as a whole applicable. The second solution could be plausible as, since the criterion of 'use of equipement' is dropped, this could possibly be replaced by the idea of making the Regulation applicable as soon as data are processed by a processor established in the Union.

The consequences of the latter, however are awkward. First, this interpretation would lead to a very important extraterritorial extension of the Regulation. Any controller in the world, e.g., a controller established in Russia, would have to respect European data protection legislation, because the controller decides to involve a processor for its IT processes established in one of the Member States. This unsatisfactory result was also already mentioned and – in our opinion wrongly defended - by the Article 29 Working Group in relation with the interpretation of Art. 4(1)(c) of equipment.[60] Processors are not the same as equipment. Enforceability and jurisdiction would also really become an issue. Thirdly, this would also lead to a serious (competitive) disadvantage for the IT industry in Europe. Non-Union controllers would indeed not be eager to involve European IT processors (e.g., cloud or platform providers) any longer, if this would lead to rendering a full protective legislation applicable to their business carried out elsewere. Therefore, we do not believe that Article 3.1 GDPR should be read that once a processor of a non-Union controller is established in the Union and processes data on behalf of this non-Union controller data of (in most cases non-Union) data subjects, the whole of all provisions of the Regulation would apply.

This would also be against the idea of 'fair competition in a globalised world' as Vice President of the Commission Viviane Reding mentioned in her speech of 4 March 2014.[61] Rather only the provisions applicable to processors apply 'to the processing of

[57] See e.g., Art. 28 (3) (f) GDPR stating that the processor shall assist the controller with compliance of the Articles 32-36 (including the data protection impact assessment).

[58] See the comments of the MEP member and rapporteur J. Albrecht, Committee on Civil Liberties, Justice and Home Affiars, meeting of 15.7.2015, available at http://www.europarl.europa.eu/news/en/news-room/content/20150710IPR79917/html/Committee-on-Civil-Liberties-Justice-Home-Affairs-meeting-15072015-(a.m.) (see after around 3:12 hours).

[59] See Art. 29 WG, Opinion on Applicable law, 2010, p. 25.

[60] See *below* and Art. 29 WG, Opinion on Applicable law, 2010, pp. 21-22 and the proposed solution of the Article 29 Working Group relating to the criterion of equipment on pp. 31-32, in particular to keep the criterion but 'in a residual form' and to foresee that only certain data protection principles would apply; see also Article 29 Working Party, *Opinion 5/2012 on Cloud Computing*, 6.7.2012, WP 196, p. 7 stating that a cloud provider located in the EEA 'exports the data protection legislation to the client'. See also Article 29 Working Party, *Update of Opinion 8/2010 on applicable law in the light of the CJEU judgement in Google Spain*, 16.12.2015, WP 179 update, which however does not modify our findings on the 'use of equipment' test, as this was not addressed (also not in Google Spain 2014).

[61] See also reference to this speech by Ms. Reding, although with a different approach, by D. J. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot underming the regulation', *IDPL* 2015, advance access publication, p. 5.

personal data' by that processor. This seems more logical. It is also confirmed by the previous wording of Article 3.2 GDPR in the sense that processor was in this Article in the text of the Commission and of the Council not mentioned and where the Presidency suggested to maintain the Council's General Approach.[62] Let us take Article 3.1 GDPR and the example of a (research) platform developed in the Union, but controlled by a controller not established in the Union. If the platform would be operated by a processor in the Union (in the context of its activities), would this render the whole data protection Regulation applicable to the processing activities of the controller outside the Union or only those provisions of the Regulation applicable to processors ?

4.3 What about Article 3.1 GDPR and sub-processors?

Another question is if Article 3.1 GPDR means to include sub-processors. It is not difficult to imagine a similar situation of a research platform, where both the controller and (main) processor are located outside the Union. While the (main) processor would operate the platform for the controller, it is quite possible that the processor subcontracts some of the tasks to a sub-processor, located in the Union. With sub-processor, we refer to a party in a contractual relationship with a processor who delegates some of its responsibilites to the sub-processor.

The term and concept of 'sub-processor' as such is also in the data protection legislation recognized, for example in relation to onward data transfers.[63] The concept is now also mentioned in some way in Article 26 GDPR, requiring that the processor cannot 'enlist' another processor without prior permission of the controller.[64]

As 'sub-processor' is not mentioned in Article 3.1GPDR, and no services are directed or data subjects monitored, could the (whole) GPDR apply in the situation only the sub-processor would be established in the Union ? This is in our view unlikely, also in view of the previous understanding of the obligations of processors. Or, although not expressly provided for in Article 3 (1) GPDR, should this Article be read as also including sub-processor(s), but then only for the obligations of the (sub-)processor ?[65] This is more plausible. [66]

The new Article 3 GDPR also poses problems in case controllers or processors are *not* established in the EU, using data of data subjects for their own purposes (e.g., research) or for rendering services to parties other than the data subjects. We will explain this *below*.

[62] See Council of the European Union, Interinstitutional File 2012/0011 (COD), 10366/15, 2.7.2015, p. 35.
[63] See, e.g., in relation with the contractual clauses for transfer of data to third countries, Article 29 Working Party, Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor", WP214, 21.3.2014, and more particularly also on p. 4.
[64] See Art. 26.2 GDPR and Art. 26.4 GDPR.
[65] This is hinted at in Art. 26.4 GDPR. stating that the same data protection obligations as set out in the contract between the controller and the processor shall be imposed, in particular the implementation of appropriate technical and organisational measures. There is no reference to the applicable law.
[66] See the text as amended by the Council in (the formerly numbered) Art. 26 (2a) GDPR. The Council added that in the case another processor was enlisted, 'the same data protection obligations as set out in the contract or other legal act between the controller and the processor (…) shall be imposed', 'in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Regulation', with joint liability in case of failure.

5 Article 3.2 GDPR and the collection and use of research data of data subjects in the Union

5.1 About 'the use of equipment'[67]

As we already explained, not only mobile applications, which can be downloaded from a webstore platform or website on the Internet, but also all kinds of equipment and consumer technology, including wearables such as smart wristbands and watches and sensors on smart devices, are used to automatically collect information from data subjects in the Union. This information is often collected by non-Union companies.[68] More than a decade ago, similarly new trends of personal information collection emerged, but then via websites. The question rose then equally whether the European data protection legislation applied. At that time, a debate rose about the interpretation of 'the use of equipment' as mentioned in Article 4(1)(c), rendering the European data protection legislation applicable to non-Union companies collecting information from data subjects in the Union through such websites.[69]

The Data Protection Authorities (DPAs) played an important role in the interpretation of the present legal framework. The group of DPAs in the Union, the so-called Article 29 Working Party ('Group'), also reviewed this notion of 'equipment' in the context of on-line data protection in 2000 and data processing by non-EU based web sites in 2002. They concluded for example that if cookies sent by non-EU websites and stored on the hard disk of a computer of visitors are used for the collection of personal data, national law of the Member State where the user's computer is located, applies.[70] While this interpretation of cookies as 'means' or 'equipment' may have seemed back in 2000 quite surprising and to some too extensive, we defend this interpretation under Artikel 4.1(c) as the protection of the data subjects is the final aim of the Directive 95/46/EC[71]. The protection of the data subjects is also surfacing clearly in the recent decisions of the ECJ. The Group referred to this analysis later in its Opinion 1/2008 related to search engines. The Group therein explained that equipment could be data centres stored on the territory of a Member State, but also personal computers, terminals and servers. It is hereby important that the controller 'makes use of this equipment' or 'disposes over the user's equipment and that this equimpent is not used only for purposes of transit'.[72] At the same time, the Group clarified in its Opinion 8/2010 on applicable law, that 'equipment' could be understood as 'means' and that 'it is not necessary for the controller to exercise ownership or full control over such equipment for the processing to fall within the scope of the Directive'.[73] The Group hence comes to a 'broad interpretation of the criterion', including 'human and/or technical intermediaries, such as

[67] Note that both the terms ‚means' and ‚equipment' are used in the various official translations of the Directive 95/46/EC. See on this aspect, also Moerel, Long Arm, 2011, p. 33. 'Means' has arguably a broader scope and appears in most national implementation law, but as both terms appear in the official versions, we do not further expand on this. In this contribution, we use both terms substituting one another, without particular intention.

[68] Examples include https://jawbone.com/ ; see also the EM-Sense prototype smartwatch developed by Disney Research and Carnegie Mellon University, armed with electromagnetic sensors, telling what data subjects are touching.

[69] About the interpretation of this Article and 'equipment', see also Korff, Study on Implementation, 2002 and Moerel, Long Arm, 2011, as mentioned *above*.

[70] Article 29 Working Party, Working Document non-EU based websites, 2002, p. 11. See also Article 29 Working Party, *Working Document Privacy on the Internet. An Integrated approach to on-line Data Protection*, 21.11.2000, WP 37, p. 28, where the 'text file installed on the hard drive of a computer', named 'cookies', is used to collect data and was designated the means.

[71] Contra: Moerel, Long Arm, 2011. The author does not agree with the 'creative turn indeed to transform the territoriality principle into the protection principle'.

[72] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines*, 4.4.2008, WP 148, p. 11.

[73] Art. 29 WG, Opinion on Applicable law, 2010, p. 20. See also Article 29 Working Party, *Opinion 1/2010 on the concepts of „controller" and „processor"*,16.2.2010, WP 169, p. 26 ('Art. 29 WG, Opinion on controller and processor, 2010').

surveys or inquiries'. It states that 'it applies to the collection of information using questionnaires, which is the case, for instance, in some pharmaceutical trials'.[74] With online questionnaires, mobile apps and sensors on smart phones and wearables nowadays, it is clear that the (paper) questionnaires for collecting information[75] now have taken another form. In the light of the discussions above and in our view, platforms, understood as a whole of software code with a particular architecture and installed on IT infrastructures, would also fall under the concept of 'means' or 'equipment'. Defending a functional interpretation of 'means' or 'equipment'[76], rather than a too strict one, platforms and smart devices could in our view be interpreted as the new type of 'equipment' or 'means' which the legislator intended. The collection of (sensitive) data by sensors in wearables, through apps and sensors by mobile phones and (subsequently) by platforms, may, if collected for particular purposes other than offering or monitoring, in particular research, no longer fall under the data protection legislation.[77]

The criterion of 'use of equipment' 'situated on the territory of the said member State', 'unless such equipment is used only for purposes of transit through the territory of the Community' is clearly a physical connecting factor for rendering European data protection laws applicable whenever such equipment is used for any processing.

Recital 20 explains the purpose of Article 4(1)(c) of the Directive 95/46/EC. It reads as follows: 'Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;' The Directive 95/46/EC hence states clearly that non-EU controllers will also have to apply European data protection legislation if equipent or means are used located on EU territory, and this to avoid circumvention of the legislation.[78]

One should note that the Group tackled also the interpretation of 'equipment' in the situation where a controller is outside the Union, but relies on processors in the Union, hereby extending 'sometimes undesirable consequences of such an interpretation' whereby the controllers would have to comply with data protection law of the Member State where the processor is located. The Group highlights the unsatisfactory consequences, 'when the result is that European data protection law is applicable in case where there is a limited connection with the EU (e.g., a controller established outside the EU, processing data of non-EU residents, only using equipment in the EU).'[79] It therefore recommended the targeting of individuals approach[80], which was adopted in the GDPR, but also *to keep the criterion of equipment or means, to avoid gaps allowing 'the EU being used as a data haven'. 'The equipment/means criterion could therefore be kept, in a fundamental rights perspective, and in a residual form. It would then only*

[74] *Ibid*. p. 20.
[75] Questionnaires and terminals are the examples given in the Explanatory Memorandum to Commission, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM(92) 422 final, *OJ* C 311, 27.11.1992, pp. 30-61 ('Explanatory Memorandum'), p. 13.
[76] But: see Moerel, Long Arm, 2011. The author is defending that equipment should remain restricted to physical objects as'the drafters of the Directive had the physical location of physical objects on EU territory in mind' and holding that extending European data protection law to non-EU websites collecting information by e.g. cookies is contrary to the legislative history by the Group in its opinion of 2002 (p. 36 and p. 43). Note that even a strict interpretation would not be problematic for data collection by wearables.
[77] For the need of protection, see also e.g., EDPS, *Opinion 1/2015. Mobile health. Reconciling technological innovation with data protection*, 21.5.2015, 17 p.
[78] See also the Explanatory Memorandum.
[79] Art. 29 WG, Opinion on Applicable law, 2010, pp. 20-21.
[80] In a similar sense, see Ch. Kuner, Data Protection Law and International Jurisdiction on the Internet (Part 1&2), 18 *International Journal of Law and Information Technology* 2010.

apply as a third possibility, where the other two do not: it would address borderline cases (…) where there is a relevant infrastructure in the EU, connected with the processing of information. (…)'. The Group hence clearly suggested to keep the criterion, albeit in a residual form, foreseeing only certain data protection principles, such as the legitimacy or security measures.[81] What the Group at that time, however, could not foresee is that 'equipment' *to collect* would soon also include a vast number of smart consumer wearables. In that situation, the forementioned principles may in our opinion not be enough and all data protection principles such as information remain relevant. Collection on Union territory of personal data of data subjects in the Union therefore remains an issue.

Moreover, we do not agree that keeping the criterion of equipment/means in Article 3.2 GDPR would result in the 'undesirable consequence' mentioned above because Article 3.2 GDPR - if including again the criterion of equipment/means - limits by referring to personal data processing of data subjects *who are in the Union* the applicability of the GDPR. It is likely that due to the difficult interpretation process, the legislator has now decided to drop this criterion of 'use of equipment' all together.

But this will in our view not solve difficult interpretation issues. Moreover, the GDPR risks to open an important new gap in needed protection. We explain this with four examples below.

But first, we like to stress that the European Parliament for that reason may have also referred again to 'collection' in the wording for Recital 24 (see *above).* A mere reference in the recitals to the collection (if the EP's version would have been accepted, *quod non*), would however not have been sufficient. We therefore plead for a clear provision keeping the applicability of the legislation as such based on the equipment or means criterion, while limiting it to situations where personal data of data subjects in the Union are processed.

5.2 Research Platforms

A first example relates to the use of 'pure' research platforms, *i.e.* platforms used only for research and purposes other than the selling of goods or services. We explained that the BEAT platform allows for example to organize testing of algorithms in a wide community. The BEAT platform is open source and is likely to 'travel' around all over the world. Another example of such platform for competitions organizers for computational science is codalab.org.[82] This platform makes for a particular challenge in 2015 about 5000 face still images available with the purpose of performing automatic apparent age estimation. These types of platforms hence *need (large) data collections* (*i.e.* databases) for such use and may presumably also collect from and use these collections of data of data subjects in the Union. If these platforms are *controlled and hosted and hence located outside* the Union, the GDPR would not apply

But if such research platform *would remain in the Union*, the GDPR, and in particular the obligations in relation to the use of personal data for research, would not apply either *if controlled by a non-Union controller*. If such platform would be physically located in the Union (e.g. because the platform is hosted by a (sub)processor established in the Union, even if this would be in the cloud (in the Union)), but operated and controlled by a controller[83] established outside the Union, the data protection legislation would

[81] Art. 29 WG, Opinion on Applicable law, 2010, pp. 31-32.
[82] See Codalab.org available at https://www.codalab.org/) and ChaLearn Looking at People 2015 – Track 1 Age Estimation. About this Challenge, see https://www.codalab.org/competitions/4711 Codalab would be set up and controlled by the Outercurve Foundation (initially founded by Microsoft), with currently 'local divisions' in Algeria, Egypt, India, Japan and Pakistan. About the Outercurve Foundation, see Wikipedia, at https://en.wikipedia.org/wiki/Outercurve_Foundation
[83] E.g., a Chinese or U.S. research organisation.

currently apply[84], but, as we remark, not the GDPR as a whole. It is feasable that a (sub)processor in the Union operates the platform physically located in the Union for a controller outside the Union. The (sub)processor will typically have an agreement with the controller for rendering particular services, such as hosting the platform, uploading data collections, providing computational power, etc. The (sub)processor has under the current data protection legislation as set out under the Directive 95/46/EC only a limited set of obligations, in particular guaranteeing the security and confidentiality of processing operations and acting only on instructions from the controller.[85] The location of the (sub)processor in the Union would or should not render the full GDPR applicable to the processing of research data on the platform located in the GDPR. As we defended *above*, processors are not the same as equipment[86] as the Article 29 Working Group may erroneously have believed, and the location of the establishment of the processor should not entail rendering the GDPR in full applicable. Therefore, in this hypothesis, which is quite realistic, it remains quite uncertain whether the controller established outside the Union but using the research platform physically located in the Union as means or equipment to process personal data for research, would have to comply with the data protection legislation as set forth in the GDPR. Is it the intention of the legislator that Article 3 (1) GDPR should be read in the sense that if the controller would be established outside the Union, but contracts with an operator located in the Union to process data on its behalf, the GDPR would in full become applicable to the controller ? In other words, as we raised *above*, is Article 3.1 GDPR intended to render the whole (European) data protection legislation applicable to controllers established outside the Union, no matter whose data are processed (e.g., data of Brazilian citizens), by the mere fact that the processor is established in the Union ? If so, the location of the processors in Article 3.1 GDPR would be interpreted as an important linking factor for imposing (all) data protection obligations upon controllers outside the Union. In that case, this should be clear and its consequence should be fully understood by the IT industry in the Union. If it would not be the case, pure research platforms controlled from outside hence become islands on Union territory on which personal data processing also of data subjects in the Union is deprived from substantial European data protection, such as pseudonymisation or anonymisation of the data in case of use for research purposes.

We are sceptical that the collection by and the use of platforms could or should be qualified as processing in the context of activities of an establishment as set forth in Article 3.1 GDPR. In other words, such platforms risk in our view not to be considered 'establishments' as understood by the legislator. First, because Article 3.1 GDPR is meant for the hypothesis that the controller or processor are in the Union.[87] Second, the legislator explained its understanding of *establishment* as implying 'the effective and real exercise of activity through stable arrangements' whereby the 'legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect' (Recital 22). The legislator hereby points in our view - in the case the controller or processor is established in the Union – *quod non* in our case described above - to some representation with legal relevance of the controller

[84] see Art. 4 Directive 95/46/EC. The use of the platform by the controller would be considered 'the use of equipment' in the Union, other than for transit, rendering the Directive 95/46/EC applicable.

[85] The obligations of the processors are under the GDPR extended, but the processors still do not have the same obligations as the controllers. See, e.g., art. 5.2 GDPR, stating that (only) the controller shall be responsible for the processing principles as set forth in art. 5 GDPR and be able to demonstrate compliance therewith (lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality). See also Article 29 Working Party, *Opinion 1/2010 on the concepts of „controller" and „processor"*,16.2.2010, WP 169, p. 5, which remains however undecided about 'other consequences, either in terms of applicable law or otherwise'; about this opinion and applicable law, see also B. Van Alsenoy, 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC'.

[86] Compare also with Kuner, mentioning that 'a corporate subsidiary should not be considered to be "equipment" of the non-EU company'. Kuner, Ch., *European Data Protection Law : Corporate Compliance and Regulations*, Oxford, 2007, p. 122.

[87] See however *Google Spain* 2014 which relied nevertheless on the similar Article 4(1) in the Directive 95/46/EC and our comments on this aspect *above*.

or processor. While this could be minimal, for example by (only) one representative and the opening of a bank account, as the ECJ stated in *Weltimmo* 2015 (which however concerned a controller *in* the Union and hence Article 4(1) of the Directive 95/46/EC), smart devices which are used and spread out all over and platforms can in our view not be equaling a representation with some legal relevance of a controller or processor and hence not an establishment. Thirdly, as several controllers or processors rely on the same smart devices or platforms for the collection and processing, such sensors or platforms can hardly represent or be considered an 'establishment' of all these different controllers or processors at the same time. A broad interpretation as 'establishment' for equipment could in our view at most only fit to be used if there is only one controller or processor in the discussion. Therefore, and fourthly, as smart devices and platforms are dispersed, can be moved easily and collaborations between stakeholders using these equipments/means can easily change, such equipment could also in our views not qualify as 'stable arrangements' and therefore not fall under a broad interpretation of establishment. Finally, and for the same reasons, one could also not use the argument of being 'inextricably linked'. The ECJ used this factor to link the activities of data processing of outside the Union with activities inside the Union within a group of companies, as if they were one and the same and the processing hence coinciding with the processing taking place in the Union and withing the scope of the Directive. In the case and the data processing at hand, even the data collection in the Union for solely research purposes would not be within the scope of the GDPR and the controllers or processors outside the Union. Hence, any linking with these processing activities to render the use of the platform within the territorial scope seems possible nor useful.

Finally, if such 'pure' research platforms would be *fully and physically located outside the Union*, ànd operated by a controller (and all (sub)processors) outside the Union, neither the Directive 95/46/EC nor the GDPR would apply. But even then, there are some disturbing effects.

First, because such research platforms may have been developed in the Union. Second, there is a scale effect in that large data collections for research, which could have had their origin in the Union[88], including sometimes personal data on data subjects in the Union, are made available by these platforms. The only possible solution in such hypothesis would be contractual agreements between the owner of such platforms and the user/controller of databases located and stored with the platform, to respect European data protection legislation if research data of data subjects in the Union would be involved.

But there are more examples of data use, in particular of data *collections* in the Union by the use of equipment or infrastructures (in particular by smart devices and platforms) to which the GDPR would not apply.

5.3. Dataphilantropy

In some cases, the data subjects are willing to provide their personal data without anything in return. For example, this can be the case for particular apps or online questionnaires on particular topics or for sharing opinions. Data subjects are also willing to provide data for pure research purposes. Several initiatives exist in this regard, such as for example the Citizen Science Association.[89] In some cases, also other sensitive data may be shared by data subjects without any monitoring or expectation of any return.[90] Similar interpretation issues under Article 3.1 GDPR as discussed above in this case

[88] Such databases sometimes can merely be downloaded from the Internet. See for example, the test databases that can be downloaded from the Biometric System Laboratory of the University of Bologna, available at http://biolab.csr.unibo.it/home.asp

[89] About the European Citizen Science Association, holding its first conference in Berlin in May 2016, see http://ecsa.citizen-science.net/

[90] See, about dataphilantropy, also *above*.

remain. For example, if a processor would remain in the Union, but not the controller, would this render the collection and use subject to the whole GDPR ? What about the use of sub-processors ? Could the use of an app or online questionaire to collect information be interpreted as an 'establishment', particular in view of the wide interpretation given in recent case law, such as *Weltimmo* ? These interpretation issues however do not stand in the way of the main issue which is that if personal data are collected from data subjects in the Union by non-Union controllers (and processors) for research purposes, hence not for offering services or goods, or monitoring their behaviour, such collection escapes from the GDPR.

Such personal data collection based on dataphilantropy from data subjects in the Union, if collected by controllers or processors outside the Union, for no purposes of offering goods or services or monitoring behaviour, as we understand the term, will in our view not to be covered by the current versions of the GDPR. Monitoring is hereby in our view – and based on Recital 24 to be understood as *tracking on the Internet* (including profiling) and aimed at taking *decisions or making predictions* with regard to the data subject. This is *in many cases not the aim if data is collected and used for research*. Controllers established outside the Union may now also want to avoid such offering or monitoring. Only the European Parliament saw it somewhat broader, by referring to tracking and collection (see also *above*). This view of the European Parliament however seems not to have prevailed in the final text.

5.4 Data collections, research collaborations and platforms

As explained, research collaborations between partners who might at first sight have few things in common explode because of the availability of new tools and infrastructures and common research goals. Massive amount of data are collected and stored and can be 'mined' for new information. Platforms are a new important infrastructure element of such (research) collaborations. They also allow for network effects.[91] Data is collected on such platforms and shared amongst multiple parties. The data collection could involve the use of mobile devices and specific (mobile) applications, but increasingly include data collection through wifi infrastructure and sensors. Such data often pertains to data subjects and is also collected from data subjects in the Union, whether citizens, residents or just travellers.

Some of the partners of these research collaborations offer goods or services to the data subjects, in exchange for the data of the participants. For example, the participants enrolling for an e-coach application will get nice grafics and advice in return.[92] These partners may in some cases also process data considered to be relating to the monitoring of behaviour (see also *above*). Other partners however will also be involved, without (directly) offering such goods or services to the data subjects or monitoring them. They receive the data for data mining and further research purposes. Will the GDPR apply to these partners ? If they are not established in the Union and do not offer goods or services to the data subjects or monitor the data subject, but only use the data for further research, they will under Article 3 GDPR in principle not have to respect the Regulation. We explain this further.

Let us take the example of the collection of (health) related data through apps on the mobile phone or through smart wristbands (or watches). It is correct that data subjects will expect in many cases a service, good or something in return and that partners in the data collection will mostly not be able to collect the personal data without offering something in exchange to the data subjects. Pure altruism is still a rare good. But with

[91] See also Gawer and Cusumano, describing it as follows: 'the most critical distinguishing feature of an industry platform compared to an internal company platform or supply chain is the potential creation of network effects' in Gawer and Cusumano, Industry Platforms and Ecosystem Innovation, 2012, p. 7.

[92] About the wide variety of e-coaches, see also L. Kool, J. Timmer and R. van Est (red), *Eerlijk advies. De opkomst van de e-coach*, Rathenau Instituut, 2014, 232 p.

collaboration between several (collecting) data controllers, it may for the data subject not be clear who collects the data for research – amongst other purposes - and that this research can be done without the GDPR to apply.

Suppose that there are *two partners collecting personal data using the same app and sharing the same platform*. For the collection of the data, they could even be co-controllers as they each have their own purposes but share and determine together the essential elements of the same means[93] (for example, an (intelligent) wristband). In addition, they are likely to use also the same platform. Must the information to the data subject state which co-controller collects the data for which purpose ? The current data protection legislation is not specific on this. However, the GDPR which foresees the situation of two (or more) co-controllers does require in Article 26 GDPR that they determine in a transparent manner their respective responsibilities for compliance with the obligations under the Regulation in particular in relation to the information obligations 'by means of an arrangement between them'.[94] But the GDPR is not specific with regard to the information to be given by the co-controlers to the data subjects. Is a distinct privacy notice by each of the co-controllers required ? Probably not. Moreover, the GDPR states in Article 26.3 that the data subject may exercise its rights against each of the controllers. The Group mentioned in its Opinion on controller and processor that 'in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller's behalf'.[95] If we assume that each co-controller provides information about their distinct purposes but in the same communication, the data subject may still be willing to provide the information in return for some service by one of the co-controllers, even though the information will be used by the other co-controller for research. Does this mean that the data (co)collection by the other non-Union co-controller is subject to the GDPR ? The collection by this other co-controller does strictly speaking not relate to any service or good or monitoring offered by that same controller. Because the criterion of 'equipment' on Union territory is no longer used, and can hence not be applied to the smart devices and platforms located in the Union and used to collect information by multiple co-controllers this is no longer clear. One could defend that the collection by the co-controller B still 'relates' to or at least is connected with services or goods but these are offered by the co-controller A only. For the same reasons as stated *above*, we also do not think that this can fall under Article 3.1 GDPR as processing in the context of an establishment, not only but especially if all (co)controllers (and processors) would be outside the Union. This will remain hence a key issue. Courts will have to interprete given situations and decide without the 'equipment' criterion which allows the physical connection of the data collection and use with the territory where the personal data are collected. In the meantime, uncertainty remains.

However, it can also be *that only one partner A collects the data* but collaborates with one or more other partners B. The other partners B may than rather easily receive the data *which remain stored with the platform* and that the partner A collects (from the data subjects in exchange for something else) if the partner A mentions the finality of research in its conditions of use and the disclosure or transfer to third party recipients.[96] This third party and at the same time research partner B, could be established outside the Union, while the data remain on the platform in the Union. Technically, there is no data

[93] About the notion of co-controllers: Art. 29 WG, Opinion on controller and processor, 2010, pp. 19-20. The Group stated for example: 'When in setting up this [shared] infrastructure [to pursue their own individual purposes], these actors determine the essential elements of the means to be used, they qualify as joint data controllers – in any case to that extent - even if they do not necessarily share the same purposes'.

[94] This could also be determined by law. See Art. 26.1 GDPR.

[95] Art. 29 WG, Opinion on controller and processor, 2010, p. 22.

[96] For the processing to be ‚fair', it will be important that this information is clear and complete. See Art. 13 and 14 GDPR which now impose explicit information to the data subject on disclosure to recipients (Art. 13.1(e) GDPR and Art. 14.1(e) GDPR) and on the transfer to third countries (Art. 13.1(f) GDPR and Art. 14.1(f) GDPR).

transfer outside the Union in this case.[97] If the data subjects are informed of this use by a third party for research purposes and would validly consent with it, there could be a legal basis for the transfer and the data can be transferred from partner A for further processing by partner B, established outside the Union, while the data remain with the platform hosted in the Union. This partner B, established outside the Union, however, would not have to abide by the European data protection regulation with regard to the data collected in the Union and which stay with the platform in the Union, unless partner A would contractually impose this upon partner B. In this scenario, partner B benefits from the (massive) data collection in the Union through the application and the platform.[98] Moreover, data subjects will generally use (mobile) apps and equipment located in the Union as well to register and transfer their personal data to the platform. Non-Union controllers also often use analytic tools on Union websites to collect personal data. While under the current data protection legislation as set forth in the Directive 95/46/EC the use of these applications (e.g., analytic tool applications), apps and equipment (such as the mobile phone) in the Union for the collection and storage of the data by a non-European controller even if used for research purposes would trigger the protection of the Directive 95/46/EC, this will no longer be the same under the GDPR.

5.5 The collection and use of data of data subjects in the Union for rendering services to third parties

The gap created by leaving out the 'equipment/means' criterion as connecting factor can also be illustrated by a fourth example. Let us take the case of a controller not established in the Union using data of data subjects for *rendering services to parties other than the data subjects*. An example is a directory of data subjects, including data subjects residing in the Union, which directory can be searched and used by third parties. The data could be collected from (various) public (web)sites containing personal information of data subjects in the Union (e.g., public directories, blogs or tweets) using 'equipment'[99] by these collectors (controllers). Under the current Directive 95/46/EC, the EU data protection legislation may apply. These directories will not always be related to offering services to the data subjects themselves, especially if these data subjects are for example not aware that they are listed in such (overseas) listings (for example, and especially in case of negative listings, for example of bad debt or bad risks).

The data however would be shared or sold to third parties, for example because these third parties have an interest in using these data. The new Article 3 GDPR does not seem to apply in this case to the data collection and processing by the controller established outside the Union and also not by the second third party, if established outside the Union, although affecting data subjects in the Union.[100] If the data are collected from within the Union, hereby using automated means, one could say that such protection to the data subjects under the GDPR would be justified, as data subjects are becoming

[97] See also Art. 44 et seq. GDPR where transfer is described as transfer to a third country (or to an international organisation).

[98] See and compare with the use of so-called analytical tools for websites collecting visitor information (e.g., page views, etc) . Examples are Google Analytics, Flurry, … While the websites using these analytical tools, if established in the Union, will have to comply with data protection rules, the partner offering the tool and receiving most of the information collected from visitors on the website and used for further analytics, may not, if the data would remain on a platform in the Union. This is different, however, with the transfer of the data outside the Union, in which case the data protection rules for transfer and the need for an adequate level of protection (e.g., by standard contractual clauses, ….) will apply.

[99] Such equipment could include tools for 'scraping' information from public websites in the Union or other processing means (other than for transit). Such public websites could e.g. include health information (or health information requests).

[100] If the second third party would on its turn use the data for offering goods or sevices to data subject in the Union, this third party would have to respect the Regulation, and one could possibly also defend in this case that the first third party, if aware of this further use by the third party, would also be bound by the Regulation, as the initial collection could be interpreted as 'related' to the offering of such goods or services.

increasingly global citizens, and will be affected as they may also be doing business or want to conclude e-commerce agreements with entities established outside the Union.

A similar situation would exist if for example health related data (e.g., of a health related site where diabetes patients ask questions[101]) or facial images would be collected (scraped) for further sale for research purposes.

This need for protection could in both cases at least be defended precisely because the data were collected on Union territory from data subjects in the Union which protection is here at stake. The EP also sees this need for protection upon collection as it proposed it to include collection in Recital 24 (see *above*). Extraterritorial application may be an issue, but this is already an aspect of Article 3.2 GDPR in any case.

6 (Unintended) consequences

The European Data Protection Supervisor (EDPS) referred recently to the territorial scope of the GDPR. In its Opinion at the start of the co-decision negotiations on the GDPR in July 2015, he stated: 'The General Data Protection Regulation will potentially affect, for decades to come, all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who process personal data on individuals in the EU.' [102] In the footnote to this phrase, the EDPS however is sceptical. The EDPS states: 'The material and territorial scope of the GDPR is difficult to summarise succinctly. The institutions seem to agree, at least, that the scope covers organisations established in the EU which are responsible for processing personal data either in the EU or outside it, organisations established outside the EU who process personal data of individuals in the EU in the course of offering goods or services to or monitoring individuals in the EU. (...)'. Other uses of personal data by organisations outside the Union are hence clearly not covered.

The reasoning and arguments mentioned above, demonstrate in our view the risks of quasi unrestricted access to important (health) data of Union citizens for research purposes by entities established outside the Union through the use of smart devices and platforms and other applications without being subject to the GDPR. These entities include not only academic but also commercial and governmental organisations. This could clearly lead to a (competitve) disadvantage for entities performing research with personal data and which are not established outside the Union. They could not use any such data as received without restrictions or requirements for research purposes or testing (in particular, of coding or pseudonymisation or anonymisation) which controllers established in the Union have to respect. Moreover, data subjects in the Union do not receive data protection, although this is the aim of the GDPR.[103]

In other words, Article 3 GDPR on the territorial scope is in our view not fit for controlling and protecting the use of personal data of data subjects in the Union for research purposes, and even beyond. We demonstrated that Article 3 GDPR as it is worded now is also not adapted to the use of new types of data processing collaborations and infrastructures, such as (research) platforms. Dropping the concepts of processor (and controller), as some suggest, is in our view not required and does not offer a solution either.

---

[101] In this case, other parties may render a service of replying to these questions, but the collecting party does not render any service.

[102] EDPS, *Opinion 3/2015. Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform*, 27.7.2015, p. 3 and see footnote 7.

[103] See also Council of the European Union, Interinstitutional File 2012/0011 (COD), 10349/14, 28.5.2014, p. 2: 'During the March Council, the draft provisions as regards the territorial scope of the regulation as defined in Article 3.2 were broadly supported, highlighting the need to broadly ensure the application of Union rules to controllers not established in the EU when processing personal data of Union data subjects', available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT

When determining the desired territorial scope of data protection, it remains important to acknowledge that personal data processing may serve other purposes than the offering of goods or services to the same data subjects, for example for risk scoring or security purposes (of others) or research. Such data could be collected in the Union and the processing activities on personal data may take place in the Union but remain controlled by an entity outside. The GDPR would in that case not apply. We summarize the current Article 3 GDPR as applied to research in the Table 1 *below*. Most of the (interpretation) problems mentioned above could in our view be solved by re-instauring the physical criterion of the use of equipment/means on Union territory enabling the collection or the use of personal data of data subjects in the Union (e.g., on platforms installed in the Union) to protect these data subjects. *A physical connection criterion in particular when data are collected and processed without leaving the Union* remains in our view important. It is not because processing and storage in the cloud now is possible, that a physical connection, especially for collection purposes, would have no relevance anymore. Moreover, the interpretation issues with regard to 'equipment/means' of the past should also not stop the legislator of continuing to using the criterion, albeit with some clarification. The Group who discussed the difficulties as mentioned also clearly was not defending to delete the criterion, but to keep it (see *above*).

Table 1: Summary of the new territorial scope (Article 3 GDPR)[104]

Controller or processor **is established in the Union**	**The controller or processor is <u>not established</u> in the Union**	**<u>Controller nor processor is established</u> in the Union**
and processes personal data in the context of the activities of an establishment (in the Union)	and processes personal data *of data subjects in the Union* related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects or related to the monitoring of their behaviour (in the Union)	and (collects and) processes in the Union personal data *of data subjects who are in the Union* for archiving purposes in the public interest, or scientific or historical **research purposes,** or statistical purposes
GDPR applies	**GDPR applies**	**GDPR <u>does not</u> apply !?**

Moreover, this physical connection is also important for allowing for better defining jurisdictional aspects and proper enforcement. This also appears from the recent *Weltimmo* case[105], where the ECJ applied a broad interpretation of establishment and was definitely also concerned about the powers of the national Data Protection Authority in Hungary. A physical 'rattachement' hence remains important in European private international law, even when confronted with fast developing technologies rendering processing possible in the 'cloud'.

[104] For the text of the Proposal, as amended by the EP and the Council, including the position of the EDPS, see e.g., https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf .

[105] See also *above*.

This is also important for the use of data for research. If this would not be considered a priority, we approach another (policy and research) issue: to what extent does the use of personal data for research shall (not) be subject to the same or similar rules as for personal data processing altogether ? With the advent of new data mining techniques, new knowledge may emerge from (already available) data. Such data permitting new knowledge shouldn't it be open for re-use for research without too many restrictions or even no rules at all – not only for non-Union controllers or processor but for all ? The present article 89 GDPR already removed the need of consent as put in the texts before. Anonymization (as proposed by the Commission) or pseudonymisation (de-identification) (as proposed by the European Parliament and the Council) and which found their way in the final text of article 89 GDPR may not be fit for this purpose.[106] Could a use-based approach not be an alternative ?[107] This is another fundamental question which needs further research and investigation.

7 The way forward

The risks of research with personal data include the use and availability of massive amounts of data about individuals without appropriate safeguards for the right and freedoms of the data subjects and proper (data) protection leading to risks of re-identification (because unsufficient protective mesures or safeguards were taken) and reuse by different stakeholders for different than the initial purposes of the collection.[108] For this reason, the New Regulation imposes respect of appropriate safeguards, in particular further to a previous Council's suggestion of 'measures (…) to minimise the processing of personal data in pursuance of the proportionality and necessity principles, such as pseudonymising the data'[109] At the same time, research with personal data should remain possible. Therefore, various derogations from data protection obligations (e.g., respecting the right to object) can be invoked, insofar as these rights 'are likely to render impossible or seriously impair the achievements of the specific purposes, and such derogations are necessary for the fulfilment of these purposes'. We defend - based on our analysis above - that in addition the rules on the territorial scope should be improved. While we have no objection to inserting the targeting approach in Article 3.2 GDPR to offer better protection, the legislator should reuse Article 4.1(c) of the present Directive and complete it with an additional factor but not replace it without due reflection.[110] We do not believe that Article 4.1(c) can be replaced and amended by only a full 'virtual nature' variation of the territoriality principle.[111] Only the criteria of (i) the processing of personal data *of data subjects in the Union*, combined with (ii) the use of *means, tools or equipment on Union territory for collection or use purposes*, can offer sufficient (data) protection for the collection and the processing of personal data of data subjects in the Union for research purposes by non-Union controllers[112]. By stressing

[106] See Art. 83 GDPR.

[107] See also Article 29 Working Party, *Statement on Statement of the WP 29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU,* 16.09.2014, WP221, p. 2.

[108] A typical example would be the reuse of data relating to health from patient records for insurance risk evaluation purposes.

[109] See amendments and text by the Council of (the as formerly numbered) Art. 83.2 GDPR. This text is not fully retained in the final text.

[110] It was initially also not the intention of the Commission to amend Art. 4.1(c). See European Commission, First Report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, pp. 16-17: 'The Commission's priority is, however, to secure the correct implementation by the Member States of the existing provision. More experience with its application and more reflection is needed, taking into account technological developments, before any proposal to change Article 4 (1) (c) might be made. Notwithstanding the need for this further reflection, it would be wrong to give the impression that the whole of Article 4 is contested. On the contrary, large areas of its application are uncontested and are the subject of unanimous agreement among all data protection authorities and the Commission.'

[111] See Moerel, Long Arm, 2011, p. 44 where the author pleads for amendment of Art. 4.1(c) 'in such a manner that it will be a true 'virtual' reflection of the territoriality principle.'

[112] And maybe other activities which we did not think of (yet).

the collection aspect, the mere use of IT, cloud or other processors on Union territory by a non-Union controller, should not export the Union legislation as a whole where this is desirable nor needed. This is also in line with the proposed amendments for Recital 24 of the EP as explained *above*. The aim of the Union legislator should remain a true concern to protect individuals on its own territory, whatever the nationality, as such in respect of fundamental rights.[113] There is no reason to abandon the territoriality principle, even in a highly complex connected, some say 'virtual' world. But nothing can be 'virtual' without processing activities somewhere on the 'ground' by some entity using some physical 'means' located somewhere. The risk of succesful forum shopping, sometimes mentioned as a risk where applicable law and jurisdiction would be based on the location of equipment, and to be avoided, is in our view limited. Reasons include the harmonized approach to be reached by the use of an instrument such as a regulation and because smart devices and platforms can be used everywhere in the Union, as a result whereof 'shopping' is hardly possible anymore. Throwing over board the 'use of equipment, automated or otherwise,' connecting factor which is based on the well established and proven useful principle of territoriality, also in terms of jurisdiction, is throwing 'the baby out with the bathwater'. It would be against all good intentions if the Union would become a data heaven for collecting and processing personal research data by non-Union entities.

One possible remedy would be to add in Article 3.2 GDPR a new alinea (c) stating that the Regulation applies (…) where the processing activities are related to '(c) processing of personal data of data subjects in the Union for archiving in the public interest, historical and scientific research purposes, or statistical purposes'. However, when completing Article 3.2 GDPR in this way, this may extend the application field of the GDPR to the use of all data for archiving in the public interest, historical and scientific research purposes, or statistical purposes even if collected outside the Union. As this is not realistic, we are not in favor of this fix.

Another possible remedy would be to re-instate in Article 3.2 GDPR a new alinea (c) with the criterion of *the use of equipment or means located on Union territory* (other than for transit). In this way, this provision would cover all personal data processing, including (most importantly) *collection*, of data subjects in the Union through equipment or means, on the territory of the Union. It is important to note that any adverse effect by a too broad application scope of this linking factor as currently may be the case under the Directive 95/46/EC and for which the Article 29 Group warned, is not present. In Article 3.2 GDPR, there is already the requirement that the processing shall be 'of personal data 'of data subject in the Union', contrary to the present text of Article 4.1(c) Directive. This limits the scope sufficiently and avoids that if a processing by a non-Union controller merely takes place in the Union through a processor and would only concern non-Union data subject, the Regulation would apply, which would be a too far reaching measure.[114] In other words, by further connecting the criterion of 'equipment' with the collection and processing of Union data subjects' data, possibly by also referring to the collection and to research purposes, the gap will be closed without stretching the scope too far. The issue is however how equipment should be understood. Various interpretations exist (see *above*) and in this case we would recommend to also describe or define the concept, as also including apps and wearables and in particular platforms as the collection of data by sensors and platforms and the use of these data on platforms - contrary to website on which data subjects fill out information - may be less obvious or more 'hidden' for the data subjects.[115]

[113] See also the reasoning by Art. 29 WG, Working Document non-EU based websites, 2002, p. 5
[114] See also *above*.
[115] For example, it should be described as also including, without limitation, collection by cookies, by wearables and sensors and platforms. About the need to (have) define(d) 'equipment', see in the same sense, Moerel, Long Arm, 2011.

The third option would be to maintain the personal data processing of data subjects in the Union but to drop the further specification of the intended uses of the data by the controller. After all, the intended uses of the personal data seem to belong rather to the material scope than to the territorial scope. Article 3.2 of the GDPR would then state as follows: 'This Regulation applies 'to the processing of personal data *of data subjects in the Union* by a controller (or processor[116]) not established in the Union'.[117] The emphasis is hence on the processing of personal data as soon as it concerns individuals, data subjects, who are present or reside in the Union. This option however necessarily leads to an extra-territorial application of the data protection legislation. This is not evident, and control and enforcement remain an issue as well.

This brings us back to inserting 'the use of equipment' in the Union, connected with the collection and processing of Union data subjects' data as the better option. This would necessarily also entail the adoption of the previous interpretations of the term 'equipment' and clarifications in this regard. This solution would be preferable from a legal certainty point of view rather than some clarification in Recital 24 which the European Parliament previously proposed and which also refered to collection and broadens montoring. Mere reference to collection (by any equipment), however, is in our view too narrow. Platforms may also enable the mere use of personal data collections of data subjects in the Union.

Conclusions

Replacing the 'use of equipment (…) situated on the territory' criterion by two new provisions in the GDPR deploying use oriented criteria merely aiming at catching the use and processing of personal data for (commercial) purposes of offering goods or services or (behavioural) monitoring does not address the use for research purposes. Research typically would not be interested in the use of personal data for directing and often also not in monitoring behaviour (on the Internet).

We argued that by leaving out the criterion of 'equipment' from the provisons on the territorial scope provisions as now mentioned in Article 4(1)(c) Directive 95/46/EC, a controller not established in the Union would be allowed to collect and/or to use any information about data subjects in the Union with any equipment, such as platforms, for research purposes which would not fall under offering goods or services or monitoring without having to respect the GDPR. The data collection could be done from sensors, from public sites, or in collaboration with other parties organized in particular on and around platforms. We discussed four scenarios, enabling the collection, storage and use of large amounts of data for scientific and research purposes by entities from outside the Union which will not be subject to Union data protection law. This risks in our view to remain the case even taking into account the wide interpretation given to 'establishment' by the ECJ in the most recent caselaw. These non-Union entities may have a competitive advantage in being not restricted in the use of personal data collected and used for research in the Union under the Union data protection legislation as compared to research organisations established in the Union.

We therefore plead for a sharper determination of the territorial scope of the GDPR, by a clear physical attachement factor, *i.e.* the use and place of processing equipment/means in the Union, not only for collection but also for the use, in case the controller is not established in the Union for the processing of Union's data subjects' data. We plead for

[116] See amendment 97 by the European Parliament to Art. 3.2. This need to add 'or processor'does not seem to be justified, since a processor would only be subject to limited obligations (see *above*) and not to the whole set of obligations.
[117] See also with a similar suggestion: R. Polčák, 'Getting European Data Protection Off the Ground', *International Data Privacy Law,* Advance Access published, 1.10.2014, p. 8.

clear terminology as well: does processor include subprocessors in article 3.1 GDPR ? And which obligations under GDPR apply if the processor(s) are established in the Union ? With new infrastructures, such as platforms, and data collection strategies becoming increasingly important, the legislator should keep several hypothesises in mind and deploy sufficiently broad criteria 'in the light of the objective (…) consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules'.[118]

This physical connection remains also important for allowing a better definition of the jurisdictional aspects and proper enforcement. Althought there have been discussion in the past on how to interprete 'equipment', such by including cookies, these interpretations could in our view still hold. Without clear criteria, stakeholders will face again long procedures about territorial application. This is not at all good for legal certainty.

This article has received funding from the European Community's 7th Framework Programme in the context of the BEAT project under grant agreement no 284989. The author also thanks Brendan Van Alsenoy and Fanny Coudert of CiTip for their valuable comments. The viewpoints in this article are entirely those of the author and shall not be associated with any of the forementioned projects, persons or entities.

[118] See the ECtJ in *Weltimmo* 2015 as discussed *above.*

References

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, pp. 31- 50.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, *O.J.* L 119, pp. 1-88, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL

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), COM(2012) 11 final, 25.1.2012, 118 p.

Council of the European Union, Interinstitutional File 2012/0011 (COD), 10366/15, 2.7.2015, available at http://data.consilium.europa.eu/doc/document/ST-10366-2015-INIT/en/pdf

Council of the European Union, Interinstitutional File 2012/0011 (COD), 15321/15, *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) [first reading]– Confirmation of the final compromise with a vue to agreement*, 17.12.2015, 207 p., available at http://data.consilium.europa.eu/doc/document/ST-15321-2015-INIT/en/pdf

European Commission, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final.

EU Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe*, COM(2010)245 final, 19.5.2010, 42 p.

EDPS, *Opinion 3/2015. Europe's big opportunity. EDPS recommendations on the EU's options for data protection reform*, 27.7.2015, 12 p.

EDPS, *Opinion 1/2015. Mobile health. Reconciling technological innovation with data protection*, 21.5.2015, 17 p.

Article 29 Working Party, *Update of Opinion 8/2010 on applicable law in the light of the CJEU judgement in Google Spain*, 16.12.2015, WP 179 update, 5 p.

Article 29 Working Party, *Statement on Statement of the WP 29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 16.09.2014, WP221, 3 p.

Article 29 Working Party, *Opinion 5/2012 on Cloud Computing*, 6.7.2012, WP 196, 27 p.

Article 29 Working Party, *Opinion 8/2010 on applicable law,* 16.12.2010, WP 179, 34 p.

Article 29 Working Party, *Opinion 1/2010 on the concepts of „controller" and „processor"*,16.2..2010, WP 169, 33 p.

Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines*, 4.4.2008, WP 148, 29 p.

Article 29 Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*, 30.5.2002, WP 56, 16 p.

Article 29 Working Party, *Working Document Privacy on the Internet. An Integrated approach to on-line Data Protection*, 21.11.2000, WP 37, 99 p.

ECJ, C-131/12, *Google Spain SL, Google Inc. v. AEPD, Gonzalez*, 13.5.2014

ECJ, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* 6.10.2015

ECJ, C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabads ág Hatóság* , 1.10.2015

Vz. Rb. Eerste Aanleg, *Debeuckelaere v. Facebook Inc., BVBA Facebook Belgium and Facebook Ireland Limited*, 9.11.2015, available at https://www.privacycommission.be/nl/nieuws/het-vonnis-de-zaak-facebook

Bygrave, L., *Data Privacy Law: An International Perspective*, Oxford, Oxford, 2014.

Kuner, Ch., *European Data Protection Law : Corporate Compliance and Regulations*, Oxford, 2007.

Kool, L., Timmer, J. and van Est, R. (red), *Eerlijk advies. De opkomst van de e-coach*, Rathenau Instituut, 2014, 232 p.

Gawer, A. and Cusumano, M., *Industry Platforms and Ecosystem Innovation*, 2012, 27 p. available at file:///C:/Users/Gebruiker/Downloads/98590.pdf

Gawer, A. (ed.), *Platforms, Markets and Innovation*, Cheltenham (U.K.), Northhampton (MA, U.S.A.), Elgar, 2011, 396 p.

Korff, D., *EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws*, Cambridge, 2002, 209 p., available at http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE

Kuner, Ch., Data Protection Law and International Jurisdiction on the Internet (Part 1), 18 *International Journal of Law and Information Technology* 2010, p. 176.

Kuner, Ch., 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', 18 *International Journal of Law and Information Technology* 2010, p. 227.

Kranenborg, H., 'Google and the Right to Be Forgotten', Case Note, *EDPL* 1, 2015 pp. 70-79

Lokke, M., 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? ', IDPL 2011, pp. 28-46.

Polčák, R., 'Getting European Data Protection Off the Ground', *IDPL*, Advance Access published, 1.10.2014, p. 8.

Svantesson, D. J., 'Extraterritoriality and targeting in EU data privacy law: the weak spot underming the regulation', *IDPL* 2015, advance access publication.

Van Alsenoy, B., 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC', ICRI Working Paper Series and *Computer Law & Security Review*, vol. 28, pp. 25-43.

Van Alsenoy, B., Kuczerawy, A. and Ausloos, J., 'Search enginges after *Google Spain*: internet@liberty or privacy@peril ?', ICRI Working Paper Series, 73 p.;

Van Alsenoy, B. and Koekkoek, M., 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'', *IDPL*, 2015, pp. 105-120