The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit

De Hert, Paul; Papakonstantinou, Vagelis

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2017.03.008

Publication date:
2017

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit

Paul de Hert [a,b,*], *Vagelis Papakonstantinou* [a,*]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *Tilburg University (TILT), The Netherlands*

Keywords:
Brexit
EU data protection
UK data protection

A B S T R A C T

The die is cast. At the time of drafting this paper the so-called Brexit, the exit of the UK from the EU, seems like a certainty after the poll results of 23 June 2016. Within such historic, indeed seismic, developments data protection seems but a minor issue, a footnote to a world-changing chapter waiting to be written. Yet, from our modest vantage point, undertaken after this Journal's kind invitation, we submit that data protection, although one out of the myriad legal aspects pertaining to Brexit that urgently await consideration, may prove to be a crucial issue in this process. Notwithstanding what happens in the immediate future, when attention will presumably be focused on coordinating the dates when Brexit may potentially occur and the GDPR comes into effect, long-term thinking is critical. We believe that, because developments in this field of law will be among those felt directly by individuals on both sides of the Channel, data protection has the potential to be among the issues that "*make*" or "*break*" a possibly successful Brexit – if success is perceived as minimal disturbance to an already functioning system. UK and EU data protection are intrinsically connected by now, by osmosis, after decades of mutual exchanges and intensive collaboration. If indeed, contrary to our wishes, a data protection Brexit does take place, the preferred way forward for the authors would be for the UK to unreservedly and permanently adhere to the EU data protection model. If this will not be the case, then we feel that a high-level principle-driven solution would serve data protection purposes better than a detailed and technical solution; the latter, if ever achievable, would essentially attempt the impossible: to surgically severe what is today an integral part of a living and functioning system.

* *Corresponding authors*. Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussels, Belgium.
E-mail addresses: paul.de.hert@vub.ac.be, paul.de.hert@uvt.nl (P. de Hert); vpapakonstantinou@mplegal.gr (V. Papakonstantinou).
http://dx.doi.org/10.1016/j.clsr.2017.03.008

1. Introduction: how to execute the delicate operation of Brexit?

The die is cast. At the time of drafting this paper the so-called Brexit, the exit of the UK from the EU, seems like a certainty after the poll results of 23 June 2016. Within such historic, indeed seismic, developments data protection seems but a minor issue, a footnote to a world-changing chapter waiting to be written. Yet, from our modest vantage point, undertaken after this Journal's kind invitation, we submit that data protection, although one out of the myriad legal aspects pertaining to Brexit that urgently await consideration, may prove to be a crucial issue in this process, a potential breaking or making point that could function either way: ignite separation feelings or evidence brotherly love that however needs to be viewed from now on under a different perspective.

The reasons why we believe that data protection may hold this role pertain to its nature. Unlike other EU legislation that is usually too technical and, although affecting profoundly whole areas of law, its effect may not be directly felt by the masses, data protection has over the years developed a direct effect over individuals. Despite being frequently confused with privacy, something inexcusable under EU nomenclature, the fact remains that individuals do care deeply today, how their personal data is being processed. EU data protection law in one way or another directly affects that within EU borders; in fact, the field has grown to be listed among these where the EU guides the world, at least in the sense of actively exporting a formal regulatory model.[1] The UK is currently found at the epicenter of this process, co-shaping data protection at EU level while applying EU rules and regulations locally. Given the interplay of this relationship, both Britons and EU citizens will be directly affected by the UK's official stance on data protection, whenever this is crystallized.

The same is the case at data controller level. The UK's approach to data protection in the future will directly affect the way they do business today. In cases where they belong to the public sector or are even law enforcement agencies, the issue is whether they will achieve any cooperation on their respective fields of activities from their neighbors. Within a globalized, internet environment, this is a crucial option. Finally, even lawmakers will be affected: data protection, at least in Europe, is embedded into national law, its provisions to be found in all types of unrelated laws and regulations, after some fifty years of active and rigorous implementation. The UK's policy decisions, to change or keep all that, may not only cause substantial new law-making work but might also create new legal tools of cooperation on each side of the channel.

This paper is not aimed at speculating on an uncertain future, meaning on how exactly the relationship between the UK and the EU in the data protection field will develop under Brexit circumstances. Such a task would be wildly speculative, given that no constants whatsoever for this legal exercise are known today. Neither is this paper intended to constitute an historical assessment of the UK's involvement into EU data protection laws, before and after the introduction of the EU Data Protection Directive. A detailed comparative law analysis would be necessary in that regard; its time has, arguably, not yet come. Instead, this paper aims at highlighting certain aspects in the EU and UK data protection relationship, so as to assist lawmakers as best as possible in their difficult task of devising the legal tools through which to execute the delicate operation of Brexit in the data protection field. Our paper will also engage in a form of wishful thinking, identifying what will be sorely missed in EU data protection in the event of a Brexit, and hope that things were, or become, otherwise.

2. The UK and EU data protection: a late-starter turned into a late bloomer

The UK has been recorded in data protection history as an unwilling entry in the field. Its first Data Protection Act was released in 1984, relatively late in global terms of comparison. This reluctance was by no means caused by lack of interest. Indeed, the first "data surveillance bill" was introduced in the UK, unsuccessfully, as early as in 1961.[2] Subsequently, two comprehensive reports were released during the 1970s on the matter, by the Younger[3] and the Lindop[4] committees in 1972 and 1978 respectively.[5] Notwithstanding technological developments, the reports form even today useful reading. However, the (then conservative) UK government was slow to respond.[6] It finally did so only in 1982; the relevant bill was finalized on 12 July 1984. As noted by Lloyd:

> *In commending the first Data Protection Bill to the House of Commons the Home Secretary commented that it was designed "to meet public concern, to bring us into step with Europe and to protect our international, commercial and trading interests". Whilst undoubtedly civil libertarian concerns are fundamental to the concept of data protection it is significant that these represented only one out of five interests identified and that, at least numerically, commercial and trading factors assumed greater significance. One reason for this can be seen in a letter to "The Times" from a leading industrialist arguing that: Lack of computer privacy legislation may seriously affect our overseas trade. Of the nine EEC countries only Italy, Ireland and the United Kingdom have no laws or firm legislative programme. Britain is regarded as be-*

[1] See Bradford A, *The Brussels Effect*, Northwestern University Law Review, Vol. 107, No. 1, 2012, pp. 22ff. See also Newman A, *Protectors of Privacy: Regulating Personal Data in the Global Economy*, Cornell University Press, 2008; Bamberger K, Mulligan D, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, The George Washington Law Review, Vol. 81, No. 5, August 2013, p. 1542.

[2] See Reed C, *Computer Law*, Oxford University Press, 2012, p. 469. This effort, as well as others that succeeded it during the same decade, were more of a "campaign nature" raised by individuals MPs than organized governmental attempts for the UK to acquire national legislation in this field, see Bennett C, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006, p. 84.

[3] Younger K, *Report of the Committee on privacy*, Cmnd. 5012, Her Majesty's Stationery Office, London 1972.

[4] Sir Lindop N, Report of the Committee on Data Protection, London: HMSO, 1978.

[5] See Lloyd I, Information Technology Law, Oxford University Press, second edition, 2004, pp. 38ff.

[6] Allegedly, considering this an issue on Labour party and civil rights groups agendas, see Bennett C, *ibid*, p. 90.

coming a "pirate offshore data haven" by countries that have legislated on computer privacy.[7]

Continued concern was therefore expressed at the possibility that privacy considerations might serve as a smokescreen for the imposition of data sanctions against the UK.[8]

In the same context, the first British Data Protection Act's scope was limited to "*information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose*",[9] strictly corresponding thus to the scope of the Council's Convention no. 108,[10] as after all also denoted in its title.[11] Consequently, it was a variety of reasons, perhaps commercial ones being ranked high among them, which led to its introduction in 1984. According to Bennett, "*in the final analysis, the British Data Protection Act of 1984 was passed for economic rather than for civil libertarian reasons*".[12]

The global environment at that time also needs to be kept in mind. Other equally technologically developed countries experimented with data protection laws since the 1970s. In fact, the first Data Protection Act was enacted in the German state of Hesse as early as in 1970, while Germany itself at federal level got its first Data Protection Act in 1976; France did the same in 1978; Sweden, even earlier than that, in 1973; the USA itself, despite future unwillingness demonstrable even today, acquired its Privacy Act in 1974. The seminal court decision of the German High Court on the right of self-determination was released in 1984. At the same time, at international organizations' level, by 1984, both the Council of Europe Convention no. 108 and the OECD Guidelines[13] were released; work within these organizations had begun as early as in the early 1970s. Consequently, within its league, by 1984 the UK was a data protection late-starter.

Once however in the club of data protection haves, the UK was turned into a data protection enthusiast. At international level, the UK was among the only six of the Community Member States that by 1990 had ratified the Council's Convention no. 108.[14] Today, it participates at global initiatives, such as GPEN,[15] and helped establish a network of Commonwealth privacy regulators "*to promote cross-border co-operation and build capacity for effective data protection*".[16] In the same context, acknowledging the importance of global cooperation, the British data protection authority, the ICO, released, together with its Canadian counterpart, an "Enforcement Cooperation Handbook".[17] At EU level, the UK complied in time with the Directive's 95/46 deadline for Member State implementation by 24 October 1998, having released its, second and still in effect today, Data Protection Act on 16 July 1998,[18] and never failed to be represented in post-Directive 95/46 legal work, at Article 29 Working Group level or elsewhere. Although cases were indeed recorded that seemed to be blockers to harmonization, such as for example the Durant case,[19] the UK, most notably through its data protection authority, the Information Commissioner's Office (the ICO), overall adopted a flexible and innovative approach to data protection within the given EU legal limits.

The UK's co-shaping of the EU data protection legal framework was particularly felt in the law enforcement data protection field. The UK has arguably been one of the EU countries whose personal data processing for law enforcement purposes preceded the relevant EU legal texts. UK efforts were increased after 9/11 and the terrorist attacks in London in July 2005 (and also in Madrid in 2004). From this point of view it provided useful insight (if not guidance) during the relevant law-making works at EU level. For example, the UK engaged in personal data processing for law enforcement purposes in the electronic communications field long before the 2002 introduction of the first version of the ePrivacy Directive.[20] Discussions on data retention policies, that later led to the, unlucky, Data Retention Directive,[21] took place in the UK as early as in 2000.[22] British influence was also particularly strong during the release of the 977/2008 Data Protection Framework Decision.[23]

Enthusiastic participation in co-shaping the EU data protection model does not necessarily mean wholehearted support for the notion itself. The British attitude toward data protection perhaps did not substantially vary over the years: in the relevant parliamentary debates for the passage of the 1998 Act repeated statements, this time by Labour MPs, pointed out that legislation was being introduced reluctantly in order to comply at a minimal level with "*European requirements, this time in the form of Directive 95/46*".[24] In fact, the UK approach to data protection has been, accurately to our mind, described by Bennett as "*instrumental*" (or even, if we may add, utilitarian), meaning

[7] Lloyd I, *ibid*.
[8] Lloyd I, *ibid*.
[9] See its Article 1.2.
[10] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981.
[11] "An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information", see also Gonzalez Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014, p. 93.
[12] Bennett C, *ibid*, p. 91.
[13] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.
[14] Information from Lloyd I, *ibid*, p. 53.
[15] The Global Privacy Enforcement Network, https://www.privacyenforcement.net/.
[16] Information from the ICO website, https://ico.org.uk/about-the-ico/news-and-events/current-topics/ico-helps-establish-new-commonwealth-network/.
[17] An ongoing project, lastly updated and presented at the 38th International Conference of Data Protection and Privacy Commissioners, Marrakesh, 17–20 October 2016.
[18] That, however, came into full effect only in the year 2000.
[19] *Durant v Financial Services Authority*, 2003, EWCA Civ 1746, see also Walden in Reed pp. 473ff.
[20] See Lloyd I, *Information Technology Law*, Oxford University Press, fourth edition, p. 58.
[21] Directive 2006/24/EC, declared invalid by the CJEU (joined cases C-293/12 and C-594/12).
[22] Lloyd I, *ibid*.
[23] Council Framework Decision 2008/977/JHA, 27 November 2008. See De Hert P, Papakonstantinou V, *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for*, Computer Law & Security Review, 25 (2009).
[24] Lloyd I, *ibid*, p. 75.

as a means to advance other individual rights and interests.[25] Perhaps characteristically, Sieghart, a prominent English data protection expert in 1976, phrased the UK's mentality toward data protection in terms of ensuring that the "*right*" people use the "*right*" data for the "*right*" purposes: "*The "right" data will be those that are accurate, complete, relevant and timely; the "right" purposes will be those to which the data subject expressly or impliedly agreed, or which are sanctioned by law; the "right" people will be those who need to use the data for those purposes alone*".[26] Some thirty-five years later Bamberger and Mulligan confirmed this finding through their own field research that divulged that "*US and UK privacy leaders generally framed privacy protection as a form of risk management to avoid harm to consumer expectations*" and "*often define privacy protection in terms of fairness to customers and employees and managing risk*".[27] This struck them as a stark difference with continental European views, where privacy is treated as an individual human right.[28]

We like this co-existence within Europe of different approaches and believe that the UK approach is not necessarily detrimental to the data protection purposes. In fact, quite the contrary may be the case. The EU approach has frequently been described as overly formalistic and bureaucratic, placing heavy loads upon state bureaucracies and private sector organizations. A pragmatic approach that acknowledges the fact of internal pluralism and identifies ways to address it within the EU data protection *acquis* should be considered welcome in a world where international cooperation and acceptance is crucial in warranting to individuals these exact data protection purposes.

3. The UK contribution to the field of EU data protection

While, as already noted, an assessment of the UK contribution in EU data protection both before and after Directive 95/46 is premature, and definitely exceeds the purposes of this paper, certain UK policy options on this matter are already easy to identify – and, we feel that, in light of an eminent Brexit, they need to be emphasized, because they may be sorely missed. In particular, the UK has developed over the years an innovative and flexible approach to data protection that, although perhaps not as much influential to other EU states as it may have wished, it anyway served the data protection community in opening new ways of thinking, demonstrating new possibilities, as well as, perhaps most importantly, keeping a balance between strict and formal legal requirements and information technology reality.

Innovation first and foremost came through the merging of the UK data protection authority with the office of the information officer – in other words, through the merging of the right to data protection with the right to access information. At first, the UK data protection authority named their DPA as "Registrar", a fact indicative of the British initial approach to data protection that gave emphasis to the registration requirement.[29] The Act of 1998 renamed the British supervisory authority as the "Data Protection Commissioner", a short-lived change because in 2000 the same post was finally called the "Information Commissioner". This succession of names reveals a different approach and understanding in the field, whereby data protection does not take automatic precedence but needs to be balanced against other individual rights, most notably the right to access information. While other data protection authorities did not follow this innovative approach across the EU,[30] it nevertheless constitutes a refreshing perspective against data protection experts' and authorities' reluctance to admit any counter-balancing power to their work perhaps other than the principle of proportionality.

British innovation in the field also came in the form of the Data Protection Tribunal, a specialized body to hear appeals. The Tribunal may have ceased its independent operation in 2010 but it demonstrated the need for a specialized judicial body to hear data protection complaints.[31] It also suggested a hybrid, and interesting, alternative to the DPA models usually met across the EU that are composed either by a single commissioner or by a multi-member commission. In the same context, the British data protection model provided for the self-sufficiency of its DPA, by allowing it to charge data controllers for registration. The identification of possible sources of income directly from the data protection addressees is an indispensable lesson to data protection authorities across the EU particularly within the contemporary budgetary limitations, although the UK's solution has also been characterized by Lloyd as a "*tax associated with computer ownership*"[32] as late as in 2004.

Innovation was not only confined in the UK's data protection legal texts but was also reflected in its ICO's practices. Indicatively, as early as in 1987, the British authority commissioned "*the most comprehensive survey of opinions on privacy ever conducted in Britain*",[33] something that many EU DPAs would even today feel that lies outside their scope of work. In addition, the use of codes of practice is also a significant British contribution to EU data protection. Their development was a priority since the time of the first Registrar.[34] This policy option has been vindicated in the text of the GDPR, where codes of conduct now occupy a whole section.[35]

More recently, the UK ought to apparently be credited also for the introduction of such novelties in the EU data protection model as impact assessments or certification. With regard to the former, Bamberger and Mulligan note:

[25] Bennett C, *ibid*, p. 33.
[26] Quoted by Bennett C, *ibid*.
[27] Bamberger K, Mulligan D, *Privacy on the Ground, Driving Corporate Behavior in the United States and Europe*, MIT Press, 2015, p. 12 and 6 respectively.
[28] *Ibid*, p.12.
[29] See Bennett C, *ibid*, p. 187. Indeed, it seems that the notion of registration, which was only recently abolished in EU data protection through the recently released Regulation, had British origins (*ibid*).
[30] Despite encouragement from legal research, see, for example, Vlachopoulos S, *State action transparency and personal data protection*, Sakkoulas A. publications, 2007, p. 74ff (in Greek).
[31] Albeit, only by controllers and processors, individuals had no access to it.
[32] Lloyd I, *ibid*, p. 75.
[33] Bennett C, *ibid*, p. 40.
[34] Bennett C, *ibid*, p. 190.
[35] Section 5 of Chapter V, Regulation 679/2016.

> *Privacy Impact Assessments are of extra-European in origin. The general concept of impact assessments originated in the United States and United Kingdom, in the context of efforts to increase the efficiency of regulation by ensuring fidelity to regulatory aims at minimal cost.*[36]

Similarly, the first PIA Handbook was developed in the UK and was published in December 2007.[37] In addition, the ICO was also among the first EU data protection authorities that experimented with certification in the data protection field, indeed paving the way for the final wording to be found in the GDPR respective provisions.[38]

Perhaps most importantly, the ICO complemented innovation with flexibility. As noted by Bennett, "*since the first Data Protection Registrar came into office, heavy-handed enforcement, although enabled by the relevant legal acts, was viewed as a last resort means*".[39] This finding was confirmed as late as in 2016,[40] and could be perceived as the basic characteristic of UK enforcement practices, regardless whether doubts have indeed been expressed with regard to its effectiveness.[41] However, in itself it constitutes an important and useful example to other DPAs across the EU.

4. Technical considerations while navigating toward an uncertain future

As things stand now, taking Brexit for granted and assuming a normal course of events in the following months, the relationship between the EU and the UK on data protection is already anticipated to cause problems: the GDPR will come into, automatic, effect on 25 May 2018, and if the UK invokes Article 50 TFEU any time in the near future (supposedly, some time during Spring 2017),[42] it will have two years to renegotiate its relationship with the EU, leaving anything from a few months to a whole year during this interim period to decide whether the GDPR applies to it or not. What happens next is anybody's guess. Kuner, Jerker, Svantesson, Cate, Lynskey, and Millard identify three possible future scenarios – as viewed from the UK perspective: First, the UK may request that the GDPR never enters into force within its territory. The 1998 Act would therefore continue in force until new data protection legislation is implemented. Alternatively, the UK may stall for time while awaiting the outcome of EU-UK negotiations, in the knowledge that any infringement proceedings against it for breach of its EU data protection law obligations would likely be equally protracted. On the other hand, the UK could recognize the GDPR and implement that accompanying legislative measures to be fully compliant with EU data protection law.[43] Any one of these scenarios is likely going to develop into a complex legal exercise to resolve – even under the assumption that the UK indeed "*incorporates all existing EU laws into UK law and then triggers Article 50*".[44] This is because difficulties are noted not only within the context of UK's Data Protection Act of 1998 but also with regard to its law enforcement personal data processing, that apparently has not been updated as per recent European Court of Justice case law.[45]

5. Responses to Brexit and their possible impact on the EU's data protection model

From the EU point of view, notwithstanding the difficult policy choices ahead with regard to the UK, there are a number of technical, data protection-specific issues to be addressed while considering its Brexit options. Territoriality, for example, is found high in the relevant list: given the expansive approach adopted in the GDPR[46] and the fact that many data controllers for EU citizens' data are located in the UK, if the EU chooses to enforce the relevant provisions immediately when they become effective it may cause legal conflict with UK authorities. The same is the case with Binding Corporate Rules (BCRs) that today constitute the preferred means for data exports for a number of international companies. It appears that a significant number, if not the majority of BCRs applicable today in the EU have been approved by the UK's ICO.[47] What will happen to them after a possible Brexit? May the ICO assume the role of Lead DPA under the GDPR? Alternatively, will these companies, that have already undergone the tedious process need of BCR ratification, need to find a new Lead DPA for EU data export purposes?[48]

Whichever the outcome of a possible Brexit in the data protection field, it is expected to affect in many ways not only formal EU and UK data protection but also business practices as well as the everyday lives of individuals. A number of important internet companies, that offer both B2B and B2C services throughout Europe, reside in the UK. The same is true for the financial sector as well.[49] Business managements may

[36] *Ibid*, p. 1660.
[37] *Ibid*.
[38] See ICO, What you need to know about ICO Privacy Seals, Information Commissioner's Office Blog, January 28, 2015, Articles 42 and 43 of the GDPR, and also Rodrigues R, Barnard-Wills D, de HertP, Papakonstantinou V, *The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR*, International Review of Law, Computers & Technology, Volume 30, Issue 3, 2016.
[39] *Ibid*, p. 189.
[40] See Galetta A, Kloza D, De Hert P, Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms, Phaedra II project, Deliverable 2.1, April 2016, available at http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D21_final_20160416.pdf.
[41] See Bamberger K, Mulligan D, Privacy on the Ground, p. 156.
[42] For the time being, the UK's Prime Minister announced, on 2 October 2016, that she will trigger Article 50 TFEU by April 2017.
[43] See Kuner C, Jerker D, Svantesson B, Cate F H, Lynskey O, Millard C, *The global data protection implications of 'Brexit'*, International Data Privacy Law, 2016, Vol. 6, No. 3.
[44] As per the UK's Prime Minister declared intention in an interview on 2 October 2017 (http://www.bbc.com/news/uk-37533727).
[45] See Kuner et al., *ibid*.
[46] See its Article 3.
[47] See the relevant list, at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.
[48] A question also raised by Lloyd in [2017] 33 CLSR Issue 2.
[49] In fact, fields of activity that will be affected in a direct way by a possible Brexit may also come from unexpected sources, as is, for example, the medical research field (Brexit timescale means NHS should plan for EU data laws, DigitalHealth.net, 13 October 2016, http://www.digitalhealth.net/digital_patient/48160/brexit-timescale-means-nhs-should-plan-for-eu-data-laws).

soon be faced with the dilemma, which laws to break. Their decision will in turn affect their clients, who may witness services that they customarily use today becoming unavailable or being offered under different terms and conditions. Within the UK, while the authors are in no position to identify the ways that UK internal data protection will be affected through its detachment from the EU legal edifice, we can only assume that these ways will not be insubstantial. From the EU point of view, its data protection model is equally at stake: the decision, whether to provide an "*easy way out*" for the UK or to insist on conformity in exactly the same way as with any other third country, will demonstrate the EU standpoint on data protection, meaning whether the EU will insist on its model, as mostly materialized through the GDPR, or whether it will relax its high level of protection in view of a new global reality.

6. Guidance to the EU lawmaking regarding Brexit

Given the important legal and political implications, and the difficult way ahead, we feel that the following points could perhaps shed some light on the issues at stake and possibly even assist lawmakers as best as possible in their difficult task of devising the legal tools through which to execute this delicate operation. The first point is EU-exclusive: we believe that, while the UK is free to explore all its data protection options under a Brexit mandate, the EU is faced with an inherent difficulty with regard to its negotiating mandate: Article 16 TFEU provides clear pro-data protection guidance, the EU data protection reform has just been completed after five years of controversy, and a series of other important legal texts are currently found at various stages of completion (for example, the amendment of Regulation 45/2001, the Eurojust and EPPO Regulations). In other words, the EU is in the middle of devising its next generation EU data protection model that cannot be seen undermined by its own drafters even before it is implemented. At the same time important case law repeatedly forced the EU toward warranting a higher level of protection to individuals (for instance, in the Schrems,[50] the data retention,[51] the Google Spain,[52] or the Weltimmo[53] decisions). In view of the above, it appears unlikely that the EU may offer any substantial flexibility to the UK during Brexit negotiations. Even under its best political intentions, any such decision would most likely be challenged in front of the Court that by now has made its point of view on the data protection topic clear.

Another point to be kept in mind is that data protection today is multi-faceted. Personal data processing is by now ubiquitous. It takes place continuously and simultaneously, largely unobserved until something goes wrong, in all fields of human activity. It is therefore doubtful whether custom-made, complex legal solutions, even under the best intentions of the negotiating parties, have any chance to be efficiently implemented. This is particularly relevant in the event that the EU also in the case of the United Kingdom opts for an approach similar to that implemented between the EU and the USA. Such complex legal constructions need significant resources to update and maintain, and still run the risk of being completely overturned by a court decision or by important political developments (in the form, for example, of the Snowden revelations). Under this light, we believe that a custom-made, detailed solution for the EU and UK data protection relationship would be ill advised. A blanket, comprehensive and easy to overview solution would be far preferable and practical.

The new data protection relationship need not be single-directional. The basic traits that the UK represents for EU data protection, namely innovation and flexibility, are crucial in contemporary personal data processing global conditions, and will be sorely missed if trapped within a fragmented new model. The EU is in need of a realistic, pragmatic, down-to-earth approach when it comes to its expectations on what data protection can actually achieve in today's globalized processing environment. In addition, the UK is an important global information technology hub, whose industry and know-how are useful, if not necessary, for the EU to achieve the status of a global technology player.

7. Long-term thinking needed: third country status, Switzerland or more?

The foregoing shows our belief that EU data protection has a lot to gain from a continued close relationship with the UK, whereby a bilateral exchange of ideas and legal notions continues to take place. Merely awarding to the UK a "*third country*" status, whereby an "*adequacy*" finding would only open the way for the exchange of data, would risk severing a much-needed relationship from the part of the EU.

Notwithstanding what happens in the immediate future, when attention will presumably be focused on coordinating the dates when Brexit may potentially occur and the GDPR comes into effect, long-term thinking is therefore critical. For example, it appears that the EU is currently suggesting to Switzerland a cooperation model whereby "*static*" bilateral agreements become "*dynamic*", meaning that Switzerland will have to automatically accept new developments in EU law, including both new rules and rulings by the CJEU.[54] This could well constitute the UK's future model as well. In other words, adherence, in one way or another to the GDPR by the UK within the next couple of years, no matter how it is achieved, should only be viewed as the beginning and not the end of a long trip ahead, given that the EU is not expected to stop regulating in the field.

Despite the above, it is also possible that new opportunities will arise even in such dire conditions as Brexit in the data protection field. These could namely originate from the Council

[50] *Maximillian Schrems v Data Protection Commissioner*, C-362/14.

[51] Digital Rights Ireland and Seitlinger and Others, Judgment in Joined Cases C-293/12 and C-594/12.

[52] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12).

[53] Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14.

[54] See The Economist, *The parable of Ticino*, 24 September 2016.

of Europe Convention 108. The authors have previously criticized its gradual attachment to the EU data protection model, which we feel deprives the Convention from its *raison d'etre*.[55] Its modernization process, currently under way, is only expected to move the Council of Europe data protection model closer to that of the EU and its GDPR.[56] However, Brexit could well be the much-needed catalyst for Convention 108 to emancipate itself from its EU cousin. The UK is a signatory member of the Convention 108: would adherence to its provisions but not to these of the GDPR suffice for the UK to maintain its current status with the EU, given that its data protection model today conforms anyway to EU standards? In other words, the case of the UK, after Brexit, could force the EU to grant special status to countries that have ratified Convention 108, rather than merely considering them as qualified candidates for an "*adequacy*" finding. In this way, it would be possible to finally make sense of two neighboring data protection models whose exact roles in global personal data processing remain unclear.

Evidently, if it were up to the authors to decide, Brexit in the data protection field will never take place. UK and EU data protection are intrinsically connected by now, by osmosis, after decades of mutual exchanges and intensive collaboration. After all, it is George Orwell's "*1984*" vision that all data protection proponents have been trying to escape from since the release of the first data protection legal instruments in Europe. However, this paper is based on the assumption that the outcome of the referendum is indeed enforced. In this case, a number of considerations, as outlined above, need to be taken into account while executing Brexit in the data protection field. We believe that, because developments in this field of law will be among those felt directly by individuals on both sides of the Channel, data protection has the potential to be among the issues that "*make*" or "*break*" a possibly successful Brexit – if success is perceived as minimal disturbance to an already functioning system. Given the above, if indeed contrary to our wishes a data protection Brexit does take place, the preferred way forward for the authors would be for the UK to unreservedly and permanently adhere to the EU data protection model. If this will not be the case, then we feel that a high-level principle-driven solution would serve data protection purposes better than a detailed and technical solution; the latter, if ever achievable, would essentially attempt the impossible: to surgically severe what is today an integral part of a living and functioning system.

8. Addendum

On 29 March 2017 the UK invoked Article 50.2 of the TFEU and notified the EU of its intention to withdraw from it. It did so by means of a letter, hand-delivered to the President of the European Council. Thereafter the Brexit negotiations were initiated, that are expected to take two years to conclude. At this moment it is hard to predict whether a "hard Brexit" or a more nuanced approach will be the outcome of these negotiations. A "no deal at all" option is also not to be excluded. Data protection will evidently be affected in any event. Hopefully, reason will prevail and "shared European values", among which the individual right to data protection, will be "advanced" within the context of a "comprehensive agreement" that will also allow for "detailed policy areas" – as stated at least in the UK's letter whose wording seems to leave some space for hope for the future.

[55] De Hert P, Papakonstantinou V, *The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*, Computer Law & Security Review 30 (2014).
[56] *Ibid*.