Data Protection: Issues of Legal Uncertainty Arising from the 2018 Act

October 2018

www.fmlc.org

Financial Markets Law Committee

Working Group[1]

Alan D. Meneghetti (Chair)	Katten Muchin Rosenman UK LLP
Ruth Boardman	Bird & Bird
Lawrence Brown	Simmons & Simmons LLP
Emma Burnett	CMS Cameron McKenna Nabarro Olswang LLP
Rebecca Cousin	Slaughter and May
Julian Cunningham-day	Linklaters LLP
Ian De Freitas	Farrer & Co
Paul Double, LVO	City of London Corporation
Miriam Everitt	Herbert Smith Freehills LLP
Christopher Garrett	Debevoise & Plimpton LLP
Joel Harrison	Milbank Tweed Hadley & McCloy LLP
Gareth Kristensen	Cleary Gottlieb Steen & Hamilton LLP
William Long	Sidley Austin LLP
Ryan Mackie	Credit Suisse
Richard Middleton	Association for Financial Markets in Europe
Mark Reynolds	HSBC Bank plc
Jeewon Serrato	Shearman & Sterling LLP
Gita Shivarattan	Ashurst LLP
Pulina Whitaker	Morgan Lewis & Bockius LLP
Joanna Perkins	FMLC Chief Executive
Virgilio Diniz	FMLC Project Manager
Juliana Franco	FMLC Legal Assistant

[1] Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only.

Table of Contents

1. INTRODUCTION AND EXECUTIVE SUMMARY

Introduction

1.1. The role of the Financial Markets Law Committee (the "**FMLC**") is to identify issues of legal uncertainty or misunderstanding, present and future, in the framework of the wholesale financial markets which might give rise to material risks and to consider how such issues should be addressed.

1.2. The rapid and substantial developments in technology and in the way organisations collect, store and use data relating to an identifiable individual or data subject,[2] as well as the importance of continuing international transfer of data flow for trade,[3] consumers and public services,[4] has resulted in a series of efforts to modernise and harmonise the current legal and regulatory framework for the protection of rights of data subjects.

1.3. Regulation (EU) 2016/679 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 (the "**new E.U. General Data Protection Regulation**" or the "**GDPR**") is an example of such efforts. Since 25 May 2018, it has been directly applicable in the U.K.—and will be until the U.K.'s withdrawal from the E.U. ("**Brexit**"), when is likely to be incorporated into U.K.'s domestic law under Section 3 of the European Union (Withdrawal) Act (the "**Withdrawal Act**"). In the U.K., the Data Protection Act 2018 ("**DPA 2018**") was enacted; it entered into force on 25 May 2018. The previous legal framework for data protection in the U.K. was set out by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "**1995 Directive**") and the UK Data Protection Act 1998 (the "**1998 Act**"). The GDPR and the DPA 2018 replace these pieces of legislation respectively.

---

[2] "Personal data" means any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4(1) and (2) of the GDPR).

[3] For example, HM Government has noted that the free flow of data is essential to the U.K. in future trading relationships. See, HM Government, *The exchange and protection of data—a future partnership paper*, (published on 24 August 2017) available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf See also paragraphs 4.1 and 4.2 below.

[4] See HM Government, *Framework for the U.K.-E.U. partnership—data protection*, (23 May 2018) available at: https://www.gov.uk/government/publications/framework-for-the-uk-eu-partnership-data-protection.

1.4. The DPA 2018 is designed mainly to achieve compliance with the GDPR in accordance with the U.K.'s obligations as an E.U. Member State. It also covers—in addition to general data processing—law enforcement data processing, data processing for national security purposes (including processing by the intelligence services), and regulatory oversight and enforcement.[5] The DPA 2018, the GDPR and Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (the "**Law Enforcement Directive**" or the "**LED**") are, *inter alia*, components of the legislative framework for personal data protection in the U.K. This is not an exhaustive list of rules applicable to data transfers, storage and processing; other relevant components of the data protection regime might include, for example, guidelines issued by the U.K. Information Commissioner's Office (the "**ICO**").[6]

1.5. The DPA 2018 has, however, been criticised for its length and complexity, the extent of the derogations and exemptions it contains (e.g.: Schedules 1 and 2) and of the powers it grants to HM Government—including, in particular, powers to alter the criteria for the calculation of penalties and the creation or removal of derogations relating to the processing of sensitive or criminal data without Parliamentary scrutiny.[7]

1.6. Additionally, upon Brexit, the U.K. will become—unless a ratified Withdrawal Agreement which states otherwise is reached between the E.U. and the U.K.—a "Third Country" insofar as the GDPR and data protection legislation applicable in the E.U. is concerned. Businesses and organisations in the E.U. sending personal data to the U.K. will therefore need to make arrangements to permit the U.K. lawfully to receive and process data relating to data subjects protected by the E.U. data protection legislation

---

[5] See paragraphs 2.2 and 2.22 below.

[6] The related topic of personal data gathering by intelligence services has been the subject of a report to the European Parliament—see, European Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the E.U., Volume II: field perspectives and legal update*, (October 2017), available at: http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega. This is, however, beyond the scope of this paper.

[7] For further details, see the Fourth Supplementary Memorandum prepared by the Delegated Powers and Regulatory Reform Committee of the Department for Digital, Culture, Media and Sport and the Home Office, which highlight a number of clauses in the Bill where the government would have delegated powers to legislate on data protection matters, available at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0106/18106-DPMsupplementary(4).pdf

See also, the Department for Digital, Culture, Media and Sport and the Home Office, *Data Protection Bill [HL]: Delegated Powers Memorandum*, available at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066-DPMsupplementary.pdf

post-Brexit.[8] Similarly, since the GDPR (and other E.U. data protection laws) will have been duly incorporated into U.K. domestic legislation, businesses and organisations sending personal data from the U.K. to other countries (including E.U. Member States post-Brexit) will need to have arrangements in place enabling the lawful transfer of personal data.[9]

1.7. The ICO has acknowledged that the DPA 2018 is not designed to address the U.K.'s data protection regime post-Brexit and that there may still be questions about how the GDPR would apply in the U.K. on Brexit, as well as difficulties in respect of the mechanics for the continuation of the lawful flow of personal data between the U.K. and the E.U. and/or Third Countries post-Brexit.[10]

1.8. The European Commission and the U.K. have individually mused that a ratified Withdrawal Agreement could include transitional provisions which allow personal data to continue to flow without restrictions between the E.U. and the U.K. after Brexit.[11] This has also been considered by the HM Government, in a framework for the U.K.–E.U. partnership on data protection, published in May 2018.[12] However, it is by no means guaranteed that such an Agreement will be reached and in force on Exit Day (namely, 29 March 2019).

1.9. In this context, the FMLC has established a Working Group to identify and make recommendations to illuminate or resolve, where and if possible, certain uncertainties, difficulties and concerns around the GDPR and the DPA 2018 and the impact of these uncertainties on the legal framework in the U.K. following Brexit.

1.10. Given the importance of the continuing international flow of data to businesses and authorities, this paper will focus on issues of legal uncertainty potentially hindering the

---

8 Article 45(1) of the GDPR. See also the "*Position paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date*", issued in September 2017 by the European Commission, Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 TEU, which deals with the treatment of data received prior to Brexit, available at: https://ec.europa.eu/commission/sites/beta-political/files/data_and_protection.pdf

9 Under Section 3 of the Withdrawal Act.

10 ICO's Overview of the General Data Protection Regulation, and commentary on the heretofore Bill (the DPA 2018) to the House of Lords.

11 See, for example, https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/706.htm (in particular, paragraph 113) and HM Government Technical Note on Benefits of a New Data Protection Agreement states that a binding legal agreement between the U.K. and the E.U. lower the risks of interrupted data flows, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714677/Data_Protection_Technical_Note.pdf

12 See "HM Government Framework for the U.K.-E.U. partnership – data protection", available at: https://www.gov.uk/government/publications/framework-for-the-uk-eu-partnership-data-protection

continuation of the lawful flow of personal data between the U.K., the European Economic Area ("**E.E.A**.") and/or Third Countries following Brexit, as well as on the framework and mechanics for supervision and enforcement of the data protection regimes post-Brexit. There may, however, be other issues of legal uncertainty derived from either or both the GDPR and the DPA 2018 which have not been considered in this paper.

1.11. It is not for the FMLC to comment on matters of policy or the form that future regulatory approaches, if any, should take and this paper should not be understood to constitute comments thereon.

Executive Summary

1.12. Section 2 of this paper considers the changes introduced by the GDPR and the DPA 2018 to the legal framework for data protection and provides an overview of the law as it stands following such changes. It examines, in particular, the requirements which must exist for the lawful transfer of personal data internationally. It also considers changes to the legal framework on provisions regarding cooperation and coordination between supervisory authorities, the extra-territorial effect/enforcement of the data protection regime in the E.U. and the U.K., the outright prohibition of automated decision-making and the potential overlaps between the provisions of different parts of the DPA 2018, the GDPR and the LED.

1.13. Section 3, in turn, sets out issues of legal uncertainty derived from the new regime and Brexit, under the assumption that no agreement addressing these is otherwise reached between the E.U. and the U.K. and in force on Exit Day. These may be generally described as uncertainties in respect of the framework for the lawful flow of personal data between the U.K. and Third Countries (which will include E.U. Member States) from Exit Day, as well as those derived from the overlap of competence of U.K. and E.U. supervisory authorities post-Brexit, the potential divergent interpretations and applications of the regime by different supervisory authorities, those related to the designation of an E.U. representative of controllers and/or processors, those derived from potential overlaps between provisions of different parts of the DPA 2018 and other laws, such as LED, the GDPR and the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "**MLD4**").

1.14. Section 4 then considers the potential impact of the legal uncertainties identified. The day-to-day operations of many businesses and organisations rely on the free movement

of data to and from the U.K. under certain processing arrangements, and this section outlines the ways in which these will be significantly impacted by Brexit. The paper also touches upon the ways in which the uncertainties in respect of the processing of personal data identified, if unresolved, may undermine risk management, the adequate pricing of financial products, operational continuity and the prevention of fraud.

1.15. Section 5 proposes solutions and/or mitigants to the uncertainties identified above. In particular, international cooperation mechanisms and transitional agreements between the U.K. and the E.U. could clarify many of the legal uncertainties identified. With regard to the status of the U.K. post-Brexit, the U.K. and the European Commission could consider an E.U.-U.K. Privacy Shield-type arrangement.

2. BACKGROUND AND OVERVIEW OF THE NEW DATA PROTECTION REGIME[13]

2.1. Underpinning the legislative structure surrounding the E.U. data protection regime are Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. These provide that an individual has the right to respect for private life and communications, to protection, access and rectification of personal data concerning him/her and the fair processing of that data only for specified purposes and on the basis of consent or some other legitimate basis laid down by law. For market participants in the U.K., important components of the data protection regime include the GDPR and the DPA 2018.

The GDPR Regime

2.2. The GDPR sets out the principles, the bases and the conditions for the lawful processing of personal data, introduces several changes to broaden the scope of protection and confers stronger rights on data subjects.[14] The GDPR is extra-territorial in scope: it

[13] This paper focuses on the new regime which came into force in 2018. For further information on the previous regime, see the Explanatory Note to the Data Protection Bill, which provides a general overview of the U.K. data protection legal background, including a comparison between the provisions of the 1998 Act and of the GDPR and the Bill (see pages 7-14 and 17-18), available at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066en.pdf.

[14] See Articles 5 (principles), 6 (lawful processing conditions), 7 and 8 (conditions for consent), 9 and 10 (conditions for processing of sensitive or criminal data), 22 (automated decision-making, including profiling which may significantly affect the data subject) and 44 to 48 (transfer of personal data to third countries) of the GDPR. The GDPR provides a wider definition of personal data; includes genetic and biometric data amongst those requiring further protection, introduces or strengthens (as the case may be) certain data subject rights such as the right to be informed, to be forgotten, to portability of data, and to access data, as well as enforcement mechanisms; introduces an accountability principle amongst the data protection principles; imposes specific statutory obligations on data processors (as opposed to the contractual obligations imposed by the 1998 Act); establishes higher penalties on breaches; etc.—see, for example, Articles 4, 5, 12 to 21, 28 and 77 to 84 of the GDPR, as well as guidelines published by the ICO and the E.U. Article 29 Working Party ("**WP29**") ahead of the GDPR coming into effect.

applies to controllers and processors (a) established in the E.U. and in the E.E.A.,[15] and (b) not established in the E.U. but which offer goods or services to or monitor the behaviour of data subjects in the E.U. whether or not those data subjects are E.U. citizens.[16]

2.3. The GDPR requires controllers or processors who are not established in the E.U. to designate a representative in the E.U., so that enforcement action in relation to infringements by the relevant controllers or processors may be brought against such appointed representative if enforcement action against the controller or processor proves difficult or unfeasible.[17]

2.4. Where there is more than one controller or processor, or there is both a controller and a processor involved in the processing and they are responsible for damage caused by the processing, each could be held liable for the entire damage and subsequently institute recourse proceedings against other controllers or processors involved in the same processing.[18]

Lawful transfer of personal data between the E.U. and Third Countries

2.5. Recital 101 of the GDPR states that:

> when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the

---

15 Please see: http://www.efta.int/About-EFTA/news/Incorporation-General-Data-Protection-Regulation-GDPR-EEA-Agreement-and-continued-application-Directive-9546EC-508856

16 Article 3(2) of the GDPR, and Recitals 23 and 24 of the preamble to the GDPR. "(…) [F]actors 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 [E.U.], may make it apparent that the controller envisages offering goods or services to data subjects in the [E.U.].". The guidance on Data Protection Officers issued by the Article 29 Working Party also states that "(…) the notion of monitoring is not restricted to the online environment and online tracking should only be considered as one example of monitoring the behaviour of data subjects". In the ICO's Employment Practices Code, available at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf), the concept of monitoring (in an employment context) is broad and means "(…) activities that set out to collect information about workers by keeping them under some form of observation, normally with a view to checking their performance or conduct. This could be done either directly, indirectly, perhaps by examining their work output, or by electronic means."

17 See Article 27 of the GDPR. Controllers and processors are however exempted from appointing a representative in the E.U. (a) where the processing is occasional and does not include large scale processing of special categories or personal data or of criminal conviction data and is unlikely to risk the rights of data subjects taking into account the nature of the processing; or (b) the controller or processor is a public authority or body. Article 27(5) of the GDPR states, "the designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or processor themselves". The ICO has said it will issue guidance on appointed representatives in due course. In this respect, see ICO draft consultation on "GDPR – contracts and liabilities between controllers and processors" (2017), p.24, available at: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

18 Article 82(4) and Recital 146 of the GDPR

> Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the Third Country or international organisation to controllers, processors in the same or another Third Country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

2.6. Under the GDPR, lawful transfers of personal data from the E.U. to a Third Country, which will include the U.K. post-Brexit, are essentially of two kinds. The first is that of transfers to Third Countries for which the European Commission has made an Adequacy Decision—i.e., a decision whereby the European Commission has found, *per* the provisions of Article 45 of the GDPR, that the Third Country's legal framework provides an adequate level of protection.[19] In this case, there are no additional safeguards required. The second is that of transfers to countries for which the European Commission has not made an Adequacy Decision. In this case, safeguards (one of items "b" to "f" below) are required. Therefore, transfers of personal data can be made on the basis of:

a) An Adequacy Decision by the European Commission in respect of the Third Country (see paragraphs 2.7 to 2.11 below). This includes decisions approving legally binding and enforceable instruments between public authorities or bodies, such as the E.U.–U.S. Privacy Shield. Transfers to countries with an Adequacy Decision can be made without complying with any additional transfer condition. They are however subject to constant review and may be challenged, which could result in an amendment or revocation.

[19] Article 45 of the GDPR. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection. For more information, see, European Commission, *Adequacy of the protection of personal data in non-EU countries*, available at: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

b) European Commission approved contractual clauses ("**Model Clauses**"), between the transferor and transferee.[20] Model Contracts (i.e. contracts based on the Model Clauses) are perhaps the most widely used legal instruments supporting data transfers to countries outside the E.E.A. and for many smaller businesses are the only available means of lawful transfer to Third Countries;

c) Standard data protection clauses in accordance with an examination procedure;

d) Binding Corporate Rules ("**BCRs**"), agreed by the business and approved by the competent supervisory authority;

e) An industry code of conduct approved by the competent supervisory authority, together with binding and enforceable commitments of the controller or processor in the Third Country;[21]

f) A certification mechanism approved by the competent supervisory authority, together with binding and enforceable commitments of the controller or processor in the Third Country;[22] and/or

g) Reliance on one of the derogations permitted by the GDPR, i.e., when (i) express consent is given by the data subject, (ii) the transfer is necessary for one of the reasons set out in the GDPR—e.g., for the performance of a contract (or implementation of a pre-contractual measure requested by the data subject), public interest, legal claims, or the protection of the vital interests of individuals, (iii) the transfer is made from a public register open to consultation with legitimate interests; or (vi) the transfer is a one-off non-repetitive transfer concerning a limited number of individuals, there is a compelling legitimate interest and safeguards in place, and the data subject is informed.[23]

---

[20] Articles 46(2)(c) and (d) and 93(2) of the GDPR. The Model Clauses adopted by the European Commission may be found at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. It is worth noting that, at the time this paper was published, the standard contractual clauses were themselves the subject of a challenge and await the outcome of a preliminary reference ruling of the Court of Justice of the European Union ("**CJEU**") being sought by the Irish High Court (see judgement, available at: https://dataprotection.ie/docimages/documents/Judgement3Oct17.pdf) Also see reference questions to the CJEU here: *Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CN0311

[21] Articles 40 and 46(2)(e) of the GDPR

[22] Articles 42 and 46(2)(f) of the GDPR

[23] Article 49 of the GDPR

The Adequacy Decision making process

2.7. The adequacy procedure is a relatively lengthy process. By way of example, it took 42 months for the European Commission to issue an Adequacy Decision in respect of Israel, 27 for Andorra, 17 for Argentina and four years for New Zealand.

2.8. The adoption by the European Commission of an Adequacy Decision under the GDPR involves several steps:[24] (a) a proposal from the European Commission; (b) an opinion of the European Data Protection Board ("**EDPB**"),[25] which replaced the Article 29 Data Protection Working Party under the new regime; (c) an approval from representatives of E.U. Member States; and (d) the adoption of the Adequacy Decision by the European Commission.

2.9. For an Adequacy Decision to be adopted, the relevant Third Country will have to provide a *comparable* (but not identical) level of privacy protection *essentially equivalent* to that guaranteed to data subjects in the E.U. The objective is not to mirror point by point the E.U. data protection legislation, but to ascertain whether the essential/core requirements of the Third Country framework and its effectiveness achieve comparable results.[26]

2.10. In assessing the adequacy of the level of protection in a Third Country, the European Commission will take into consideration, for example, the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments into which the Third Country or international organization has entered.[27] Thus, any assessment of a Third Country will factor at least the content of the

---

[24] See: European Commission, *Adequacy of the protection of personal data in non-EU countries*, available at: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[25] The process of obtaining a finding of adequacy under the GDPR commences with the applicant submitting the relevant documentation, correspondence and any applicable finding made by the European Commission, which is required by the EDPB in order to allow it to fulfil its task in advising the European Commission under article 70(1) (s) of the GDPR.

[26] Please refer to Case C- 362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015 (§§ 73, 74), on foot-note 21, as well as European Commission's Adequacy Decisions to date.

[27] Article 45(2) of the GDPR

applicable rules and the means by which their effective application is ensured,[28] as well as the legal framework for access by public authorities to personal data.

2.11. Once an Adequacy Decision has been granted, the European Commission is required to monitor—on an ongoing basis—developments that could affect its functioning, and a periodic review must take place at least every four years.[29] The European Commission may withdraw or suspend (without retroactive effect) an Adequacy Decision if it understands that the Third Country no longer ensures an adequate level of protection.[30]

2.12. Pending—or failing—an Adequacy Decision, businesses and organisations transferring data from the E.U. to a Third Country must ensure that they put appropriate safeguards in place (see paragraph 2.7(a) to (f) above) or rely on one of the derogations available (see paragraph 2.7(g) above).

Cross-border Processing: Supervision and Enforcement within the E.U., the one-stop-shop mechanism; and the designation of representatives of controllers or processors in the E.U. and the U.K.

2.13. The GDPR defines cross-border processing as either: (a) the processing of personal data in the context of the activities of more than one establishment if a controller or processor is established in more than one Member State; or (b) the processing of personal data in the context of activities of a single establishment of a controller or processor in the E.U. but which substantially affects or its likely to substantially affect data subjects in more than one Member State.[31] The GDPR provides for cooperation between the E.U. data protection supervisory authorities on cross-border infringements or cross-border enforcement of infringements of the GDPR in a particular E.U.

---

[28] On the latter, the Article 29 Working Party further notes that: "General provisions regarding data protection and privacy in the Third Country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to data protection must be included in the Third Country's or international organization's legal framework. These provisions have to be enforceable." (See "Adequacy Referential (updated)" and adopted on 6 February 2018, available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49724).

[29] Article 45(4) of the GDPR and Article 29 Working Party's "Adequacy Referential (updated)" and adopted on 6 February 2018, available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49724 .

[30] Article 45(3) of the GDPR

[31] See Article 4(23) of the GDPR. The GDPR defines neither "substantially" nor "affects", but the test is ultimately a subjective one that will be assessed on a case-by-case basis, and the conclusion will not be determined solely by elements such as the number of affected individuals or the number of affected E.U. Member State—see Article 29 Data Protection Working Party, "Guidelines for identifying a controller or processor's lead supervisory authority", 13 December 2016, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

jurisdiction,[32] giving authorities broad ranging powers to cooperate with each other under a newly established "consistency" or "one-stop-shop" mechanism,[33] with the principal aim of guaranteeing both greater cooperation between supervisory authorities and a consistent application of the GDPR throughout the E.U.[34]

2.14. The implementation of this new consistency mechanism will make away with the current system, where organisations established in more than one E.U. Member State are subject to the jurisdiction of the supervisory authority in each of those Member States. Through the new mechanism, a data controller or processor established in an E.U. Member State and carrying out cross-border processing of personal data within the E.U. interacts only with the supervisory authority of the E.U. Member State where its "main establishment" is located (the "**E.U. Lead Supervisory Authority**"). Other "supervisory authorities concerned" will, however, be involved in eventual investigations coordinated by the E.U. Lead Supervisory Authority.

2.15. The concept of an establishment is a broad one, and an organisation will have an establishment wherever in the E.U. it exercises any real and effective activity, even if that activity is minimal.[35] In determining whether processing is occurring "in the context of the activities of an establishment", context rather than physical location matters most.[36]

2.16. The main establishment could therefore be identified, for example, by ascertaining where the organisation's central administration within the E.U. is located, decisions about the purposes and means of the processing are taken, and/or the power to have those decisions implemented lies.[37] Accordingly, the location of the parent undertaking or operational headquarters of a pan-European group will more than likely be its main

---

32 See Articles 60 to 62 of the GDPR. Also, Recital 124 of the GDPR states that authorities "should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their member state, because data subjects residing on their territory are substantially affected or because a complaint has been lodged with them. Also where a data subject not residing in that member state has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned".

33 Articles 63 to 67 of the GDPR

34 Recital 135 to the GDPR

35 Recitals 22 and 36 to the GDPR;

36 Non-binding opinion of the Advocate-General of the Court of Justice, Case C 210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CC0210

37 Article 4(1) of the GDPR and Article 29 Data Protection Working Party. "Guidelines for identifying a controller or processor's lead supervisory authority", 13 December 2016, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

establishment, as that location will generally be the place of central administration within the E.U.[38]

2.17. The GDPR does not provide for situations where the "main establishment" of an organisation would be an undertaking established outside the E.U. whilst having one or more establishments in the E.U. The Article 29 Working Party therefore notes that:

> In these circumstances, the pragmatic way to deal with this would be for the company to designate the establishment that will act as its main establishment. This establishment must have the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets. If the company does not designate an establishment in this way, it will not be possible to designate a lead authority. Supervisory authorities will always be able to investigate further where this is appropriate.[39]

2.18. The main establishment of an organisation in the E.U. may be determined by factors such as where data processing decisions are made within the E.U., where directors with overall responsibility for the cross-border processing are located in the E.U., and/or where the controller or processor is registered as a company.[40]

2.19. Furthermore, as introduced in paragraph 2.4 above, for the purposes of Article 27 of the GDPR, and in the context of post-Brexit where activities of offering goods or services to or monitoring the behaviour of data subjects within the E.U take place, controllers and processors established in the U.K. but without any establishment in the E.U. are required to designate a representative in the E.U.

Cross-border Supervision and Enforcement amongst E.U. Member States and Third Countries

2.20. In addition to supervisory cooperation within the E.U., the GDPR also provides for the development of international cooperation mechanisms and mutual assistance with Third Countries.[41] Accordingly, the European Commission has indicated that it will develop international cooperation mechanisms for the effective enforcement of data

[38] Article 29 Working Party, *ibid.*

[39] Article 29 Working Party, *ibid.*

[40] Article 29 Working Party, *ibid.*

[41] See Article 50 of the GDPR.

protection obligations under the GDPR and other European data protection laws,[42] including through mutual assistance agreements and a possible new framework agreement for the cooperation between European data protection authorities and law enforcement authorities.[43]

Restriction on automated decision-making as an outright prohibition

2.21. Article 22(1) of the GDPR provides that, subject to one of the conditions in Article 22 (2) being satisfied, data subjects have the right not to be subject to a decision based solely on automated processing (including profiling) if that decision produces legal effects concerning the data subject or significantly affects the data subject in a similar way.[44]

Data Protection Legislation in the U.K.

2.22. As mentioned in section 1, above, the DPA 2018 forms a piece of the legislative jigsaw governing personal data protection in the U.K. The DPA 2018 aims at applying the standards of the GDPR (without reproducing its text) to the U.K., extending its application to areas not covered by (or covered by separate) E.U. laws, and setting out certain derogations and exemptions from the GDPR "*to make it work for the benefit of the UK in areas such as (…) financial services*" by replicating the provisions of the 1998 Act as far as possible.[45] It comprises four main elements:

---

[42] Such laws include Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "**Privacy and Electronic Communications Directive**") and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "**Network and Information Security Directive**").

[43] See European Commission Communication Paper on "Exchanging and Protecting Personal Data in a Globalised World", available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=41157. LED already contains rules on international data transfers and data exchanges between data protection authorities and non-E.U. law enforcement authorities, and Europol already has cooperation agreements with third parties for law enforcement purposes.

[44] The formulation used in Article 22(1) is not entirely new. Article 15(1) of the 1995 Directive provided that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

[45] See the Data Protection Bill Factsheet issued by the Department for Digital, Culture, Media & Sport, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644634/2017-09-13_Factsheet01_Bill_overview.pdf), and the Explanatory Notes and ICO's briefing to the House of Lords with commentary on the Bill. It is worth noting, however, that the DPA 2018 introduces two new criminal offences, amongst other changes.

a) General data processing: Part 2 of the DPA 2018 covers general data processing, setting out how the GDPR is implemented/applies in the U.K. context, to the extent that derogations are permitted;[46]

b) Law enforcement processing: Part 3 of the DPA 2018 implements the LED and provides a bespoke regime for the processing of personal data by competent authorities involved in law enforcement (police, prosecutors and other criminal justice agencies), and extends the LED regime to domestic processing of data by U.K. law enforcement authorities;[47]

c) Data processing for security: Part 4 of the DPA 2018 covers data processing for national security purposes, including processing by the intelligence services and regulatory oversight enforcement in line with modernised international standards and safeguards; and

d) Regulation and enforcement: Parts 5 and 6 of the DPA 2018 covers regulatory oversight and enforcement, granting additional powers for the ICO to regulate and enforce data protection laws, to impose higher administrative fines and to bring criminal proceedings against offences.

2.23. The GDPR is directly applicable in the U.K. now and will be incorporated into U.K. law under the Withdrawal Act following Brexit. Thus, the principles set out in the GDPR concerning the lawful transfer of personal data to Third Countries will be incorporated into U.K. law as of Exit Day under the Withdrawal Act and will apply to all transfers to those jurisdictions which are "Third Countries" as far as U.K. law is concerned. Those jurisdictions will then include E.U. Member States.

2.24. Meanwhile, the DPA 2018 specifically provides, in sections 72 to 78, principles which govern the international transfers of personal data to Third Countries. Subsections 73 (1)–(4) set out three conditions which a controller must meet before transferring personal data to a Third Country or international organisation. The first condition is that the transfer is made to satisfy a law enforcement function. The second condition states that the transfer must be based on an Adequacy Decision or, in the absence of

[46] The DPA 2018 allows, for example, the processing of sensitive and criminal conviction data in the absence of consent where justification exists, including to prevent unlawful acts and fraud and to support insurance processing under the substantial public interest exception further detailed in Part 2 of Schedule 1 of the DPA 2018.

[47] For the purposes of data protection in the U.K., "competent authority" means any public authority or any other person if and to the extent that the person has statutory functions for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention of threats to the public security. See Recital 11 and Article 7(3) of the LED, and Sections 30 and 31 of the DPA 2018. Schedule 7 of the DPA 2018 also lists competent authorities, including the Financial Conduct Authority ("**FCA**").

such a decision, on the existence of appropriate safeguards or, in the event neither is available, on special circumstances.[48] Finally, the third condition provides rules as to the nature and function of the parties—the controller and the intended recipient—of the international transfer.

2.25. The DPA 2018 also includes extra-territorial provisions similar to the GDPR and therefore will, accordingly, not only apply to controllers and processors established in the U.K., but also to:

a) controllers not established in the U.K. where (i) the personal data is processed in the context of activities of that establishment, (ii) the personal data relates to an individual who is in the U.K. when the processing takes place, and (iii) the purpose of the processing is to offer goods or services to (or to monitor the behaviour of) individuals in the U.K;[49] and

b) Processors not established in the U.K. where (i) the controller on whose behalf the processor acts is not established in the U.K. and the personal data is processed in the context of activities of that establishment, or (ii) the processor is not established in the U.K. and the personal data is processed in the context of activities of that establishment.[50]

2.26. The DPA 2018, however, does not include the GDPR requirement for controllers or processors who are not established in the U.K. but nonetheless subject to the U.K. Data Protection Regime to designate a representative in the U.K., which seems to mean that the GDPR requirement does not apply.[51] (There is a requirement for non-E.U. controllers and processors established in the post-Brexit U.K. to appoint representatives in the E.U. if they wish to process personal data relating to data subjects in the E.U.), and there is a requirement for controllers to appoint Data Protection Officers ("**DPOs**"), under Section 69.

2.27. Finally, the DPA 2018 provides that the ICO shall take appropriate steps to develop international cooperation mechanisms in line with the GDPR provisions mentioned in

---

48 Section 76 sets out in greater detail what these special circumstances might be.

49 See section 207(3) of the DPA 2018.

50 See section 207(3) of the DPA 2018.

51 See Schedule 6 of the DPA 2018 (in particular, paragraphs 9(d), 15(a), 16(a)(i), 23). There are, however, references to representatives in certain instances relating to enforcement action such as at section 143(9) of the DPA 2018 (information notices) which specifically refers to representatives appointed under Article 27 of the GDPR.

paragraph 2.20 above.[52] Such mutual cooperation is essential to the cross-border enforcement of the rights of data subjects located in the U.K. under the GDPR as well as to the enforcement of rights under the U.K. Data Protection Regime. In respect of law enforcement and security, the U.K. government has issued a factsheet summarising its intentions for U.K. criminal justice agencies to continue to share data with other E.U. Member States following Brexit, to tackle serious crime and threats to national security.[53] In light of this expressed intention of cooperation with E.U. authorities, it seems likely that there will be a similar level of cooperation regarding breaches of the GDPR by U.K.-established controllers or processors. Equally, the U.K. government will presumably be seeking commitments by E.U. authorities for cooperation regarding enforcement of extra-territorial breaches of the U.K. Data Protection Regime by E.U.-established controllers or processors.

2.28. The law enforcement provisions of the DPA 2018 (Part 3 – section 30) apply to competent authorities and any other person processing personal data domestically if and to the extent that such person has statutory functions for any of the law enforcement purposes.[54] Therefore, where personal data is processed with law enforcement purposes, Part 3 of the DPA 2018 applies.

2.29. Accordingly, the general data protection provisions in the GDPR and the Part 2 of the DPA 2018 apply to any other purpose which is not for law enforcement, even at the point that financial institutions pass on personal data to competent authorities for the purpose of compliance with the anti-money laundering regime.[55] The competent authority, meanwhile, is governed by the LED only when carrying out the law enforcement functions, even though the nature of the anti-money laundering regime is such that it has the potential to be at odds with the data protection regime.[56] In this

---

52 See sections 118(1), (3) and (5) and 120 of the DPA 2018.

53 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/685635/2018-03-05_Factsheet03_Bill_law_enforcement.pdf

54 Section 31 of the DPA 2018 defines law enforcement purposes as "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

55 See Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("**the Fifth Money Laundering Directive**" or "**MLD5**") which includes a new obligation on Member States to establish central mechanisms to identify holders and controllers of bank and payment accounts. This supplements the requirement, established by Directive (EU) 2015/849 (the "**Fourth Money Laundering Directive**" or "**MLD4**"), that financial institutions carry out data processing with a view to preventing the use of the financial system for the purposes of money laundering or terrorist financing. (This requirement has been implemented in the U.K. by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "**2017 AML Regulations**")),.

56 Please see Recital 11 of the LED.

regard, the ICO stated that "data protection is not, and should not be seen, as a barrier to an effective anti-money laundering and counter-terrorist financing regime".[57] Likewise, Part 2 of the DPA 2018, and the GDPR—i.e., not the LED—apply to the processing of both non-special and special categories of personal data for the purpose of compliance with by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "**2017 AML Regulations**"), as long as (a) "necessary for reasons of substantial public interest",[58] and (b) financial institutions ensure that the *manner* in which they process the personal data is also GDPR compliant (e.g., observe the "privacy by design" approach, taking into account core privacy considerations when designing policies and procedures relevant to compliance with the anti-money laundering regime and ensuring that the data is processed only for that purpose).[59]

2.30. Finally, as regards to the restriction on automated decision-making, sub-section (1) of section 14 of the DPA 2018 makes provision for purposes of Article 22(2) (b) of the GDPR, defining both:

a) a "significant decision", where it meets either the criteria set out in Article 22(1), (i.e. that it produces legal effects concerning the data subject or significantly affects the data subject in a similar way (section 14(2)); and

---

[57] Please see the ICO response to HM Treasury's consultation of the 2017 AML Regulations that (see the ICO's response to HM Treasury's consultation on Money Laundering Regulations 2017, 12 April 2017, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013938/ico-response-hmt-money-laundering-regulations-20170412.pdf

[58] Article 6(1)(e) and 9(2)(g) of the GDPR; and Sections 6, 8(c) and 10(1)(b) and 3, and Schedule 1, part 2, paragraphs 6(1)(a) and 6(2)(a) of the Data Protection Act 2018; and Regulations 41 of the 2017 AML Regulations (which we assume will be updated to replace 1998 Act references with equivalent GDPR and Data Protection Act 2018 references). Special category personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation.

[59] Principles such as the lawfulness, fairness and transparency/accuracy of processing, purpose limitation, data minimisation, storage limitation and integrity and confidentiality must be observed (see, for example, Regs. 18, 19 and 40(4) of the 2017 Regulations). For example, the 2017 Regulations take the application of enhanced customer due diligence ("**EDD**") wider than before, including to domestic politically exposed persons ("**PEPs**"), their family members and close associates. The ICO voiced concern about the compatibility of this with the data protection principles of transparency and accuracy, stating that: "In the case of family members of political party board members, it is important to note that many of these individuals will have no expectation that they will now be captured by the PEP regime and therefore subject to EDD… Accuracy is of particular concern where relevant persons will make the determination on whether an individual is related to or associated with PEP on the basis of 'publicly known information'." See the ICO's response to HM Treasury's consultation on Money Laundering Regulations 2017, 12 April 2017, available at: https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013938/ico-response-hmt-money-laundering-regulations-20170412.pdf). The ICO further recommends that financial institutions "consider safeguards to ensure that the information they are sourcing about individuals is both credible and lawfully and legitimately sourced when taken from publicly known sources". The FCA has since published guidance addressing the point, highlighting that a risk-based approach should be taken, for example: a family member or close associate of a politically exposed person may pose a lower risk if the PEP themselves poses a lower risk. To clarify, the FCA expects family or known close associates of UK PEPs to be treated as lower risk unless there are circumstances to suggest otherwise (see FCA finalised guidance 17/6, "The treatment of politically exposed persons for anti-money laundering purposes", point 2.31 - 2.35, available at: https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf).

b) a "qualifying significant decision", where it is required or authorised by law and does not satisfy either of the other two conditions in the GDPR Article 22(2) (i.e. the decision is necessary for a contract with the data subject or made with the data subject's explicit consent (section 14(3));

2.31. Moreover, where a qualifying significant decision is taken, section 14(4) requires the controller to notify the data subject and gives the data subject the right to request the controller to reconsider the decision or take a new decision not based solely on automated processing.

3. ISSUES OF LEGAL UNCERTAINTY

3.1. The section below considers legal uncertainties in respect of the general framework for the lawful flow of personal data between the U.K. and a Third Country (including E.U. Member States), under the assumption that no agreement addressing such issues is otherwise reached between the E.U. and the U.K. and is in force on Exit Day.

3.2. The section also considers issues of legal uncertainty specific to the consistency mechanism and the overlap of competence of U.K. and E.U. supervisory authorities post-Brexit, the E.U. representatives, the potential overlap between provisions of different parts of the DPA 2018 and other laws (LED, MLD4), the enforcement of the Data Protection regime in the E.U. and the U.K., and the outright prohibition on automated decision-making.

The status of the U.K. post-Brexit and international transfers

Transfer of personal data from the E.E.A. to the U.K.

3.3. Upon Brexit, unless a transitional agreement or a bespoke arrangement is implemented, the U.K. will be a Third Country from the perspective of the E.U. There is a need, then, to ensure that the level of protection of natural persons granted by the GDPR is not undermined with respect to the receipt of personal data from E.E.A countries in full compliance with the GDPR.[60]

3.4. An Adequacy Decision is arguably the best-suited GDPR mechanism (see paragraph 2.6 *ff*) to enable continuity of the lawful transfer of personal data flow from the 27 E.U.

[60] Recital 101 of the GDPR. Otherwise, parties will need to make sure appropriate safeguards and/or contractual provisions required by the GDPR (e.g.: Articles 46 to 48) are in place upon Brexit (see paragraphs 2.6 and 2.12 above).

and three E.E.A. Member States to the U.K. post-Brexit on a wholesale basis without the need to obtain any further authorisations.[61]

3.5. It seems unlikely however, that an Adequacy Decision in respect of the U.K. will be in place on Brexit date, as (a) such decisions are made in respect of Third Countries, which the U.K. will become only upon Brexit, and (b) the Adequacy Decision process can be quite lengthy.[62] It has been argued that certain deviations from the E.U. data protection framework provided for in the DPA 2018 might cause the European Commission to decide against the adequacy of the U.K. regime on the basis that they undermine the GDPR regime.[63] An Adequacy Decision is, in any event, not granted in perpetuity and any changes to the U.K. Data Protection Regime post-Brexit might cause the European Commission to reassess its decision.

3.6. Under the GDPR and absent an Adequacy Decision, any transfer of personal data which are intended for processing after transfer to a Third Country or to an international organisation shall take place, broadly, only in circumstances where either "appropriate safeguards" (Article 46) are in place or specific "derogations" (Article 49) apply. The latter are contextual, highly restricted and not intended to be generally relied upon. Thus, in the absence of an Adequacy Decision after Brexit, the U.K. and/or U.K. firms and regulators would have to have appropriate safeguards in place upon Brexit to allow data controllers and processors in the E.E.A lawfully to transfer data to entities in the U.K. The categories of appropriate safeguards are exhaustively listed in Article 46 of the GDPR. They can be put in place in the Third Country at the level of national government, regulatory authorities or by data processors and controllers but, broadly, each category of safeguard requires the cooperation of, or an authorisation by, one or more E.U. authorities. They may include, for example, "a legally binding and enforceable instrument between public authorities or bodies", "administrative arrangements between public authorities or bodies", "an approved code of conduct pursuant to Article 40…" or "subject to the authorisation from the competent supervisory authority… contractual clauses". It is unclear whether, after

---

61 See Recital 103 of the GDPR.

62 See paragraph 2.7 *ff* above.

63 These deviations include, for example, the extent of the derogations and exemptions the DPA 2018 contains (e.g.: Schedules 1 and 2) and the powers it grants to HM Government—including, in particular, powers to alter the criteria for the calculation of penalties and the creation or removal of derogations relating to the processing of sensitive or criminal data without Parliamentary scrutiny. See also paragraph 1.5 above. This might impact the Adequacy Decision under Article 45 of the GDPR which requires consideration on "(…) a wide array of issues such as the rule of law, respect for fundamental rights, and legislation on national security, public security and criminal law when it makes its decision" (Lord Ashton of Hyde, Second Reading of the Bill in the House of Lords).

Brexit, U.K. public and competent authorities will have coordinated the necessary general agreements, instruments or arrangements with authorities in the E.U. to enable the continuity of personal data transfer from data controllers/processors in the E.U. to the U.K. without the necessity of E.U. transferors implementing further safeguards and seeking authorisation in the E.U. for their transfer arrangements. Absent such arrangements at the national level, data flows may be impeded. Similar points may arise in respect of the processing of personal data by national authorities for law enforcement purposes.

3.7. Should none of these mechanisms be in place on Brexit date, it would be left to private parties to put in place other safeguards which do not depend on reciprocal arrangements between national authorities to continue lawfully transferring data from Brexit.

3.8. The European Commission has indeed highlighted that:

> Preparing for the withdrawal is not just a matter for E.U. and national authorities but also for private parties. As regards the implementation of the GDPR, and in particular the new tools for transfers to third countries (e.g. approved Codes of Conduct and approved certification mechanisms entailing binding commitments by the controllers and processors receiving the data in the third country), the Commission (Directorate-General Justice and Consumers) is working with interested parties and data protection authorities to make the best use of these new instruments. Moreover, the Commission has set up a stakeholder group comprising representatives of industry, civil society and academics, in which this topic will be discussed.[64]

3.9. Nevertheless, at present no codes of conduct or certification bodies have been approved and it is unlikely that they will be approved before Brexit. Therefore, absent or pending an Adequacy Decision for the U.K. Data Protection framework by the E.U., private parties willing to transfer data between the E.U. and the U.K. should rely on safeguards such as Model Clauses.

3.10. Currently, the validity of Model Clauses is under judicial challenge. If they are invalidated by the Court of Justice of the European Union ("**CJEU**"), many businesses in the U.K. may find themselves unable lawfully to receive or transfer personal data

[64] The European Commission's Directorate-General Justice and Consumers issued a Notice to Stakeholders on "Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection" on 9 January 2018, available at: http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245.

outside the U.K. (including the E.U.). Such invalidation would mean organisations would need to work out a new mechanism for transferring data outside of the E.E.A to any of the vast majority of countries that are not adequate for the purposes of E.U. law. Accordingly, there are two types of legal uncertainty. The first is whether Model Clauses are valid; the second is how the U.K. would implement new and/or temporary mechanisms.

Transfer of personal data from the U.K. to Third Countries

3.11. As mentioned above, the GDPR requirements for the lawful transfer of personal data to Third Countries (including E.E.A. countries post-Brexit) applies to U.K. organisations under the DPA 2018 framework and, therefore, the same uncertainties identified in paragraphs 3.3 to 3.9 above apply to the transfer of personal data from the U.K. to other jurisdictions.[65]

3.12. It is impossible, at this stage, to estimate the length of a U.K. Adequacy Decision process, given that there is no precedent for such a decision. It is probable that the U.K. will grant Adequacy Decisions to E.E.A. jurisdictions, given that the U.K. has implemented the GDPR into its national legislation and a decision otherwise would undoubtedly impact U.K. businesses and a future Adequacy Decision of the European Commission in respect of the U.K. This is, however, by no means guaranteed.

3.13. Moreover, post-Brexit the U.K. could introduce an independent system of adequacy, under which the U.K would decide whether a Third Country is adequate. This would be straightforward if the U.K. made the same decisions as the European Commission has already made. On the other hand, if the U.K. were to decide that a "new" Third Country is adequate that could lead to uncertainty, because it would result in transfers of E.U. citizens personal data to that "new" country via the U.K., and that in turn could cause the European Commission to review whether the U.K itself is adequate (assuming there would be an Adequacy Decision in place from the E.U. to the U.K. legal framework).

The E.U. consistency (or one-stop-shop) mechanism—the overlap of competence of U.K. and E.U. supervisory authorities post-Brexit

3.14. While the GDPR's approach to cooperation and consistency aims to streamline the European data protection framework,[66] it has also created a certain amount of

[65] See sections 73 to 78 of the DPA 2018, and paragraph 3.23 and subsequent above.

[66] See articles 3(2)(a) and 3(2)(b) of the GDPR and paragraphs 2.15 to 2.17 above.

uncertainty, most notably in relation to how cooperation and consistency will actually be achieved in practice, and indeed how the one-stop-shop mechanism will operate. Uncertainties may arise, in particular, when businesses are established in the U.K. and offer goods or services to (or monitoring the behaviour of) individuals in the E.U. (or vice-versa) post-Brexit.[67] These are outlined in the following paragraphs:

a) Data controllers (or processors) established in the U.K. with no establishment in the E.U.: it is uncertain whether such businesses would benefit from the one-stop-shop mechanism, which in theory applies to organisations with at least one establishment in the E.U. If not, such businesses will have to deal directly with the supervisory authority of each E.U. Member State into which it offers services and goods (or monitors individuals), facing not only a complex network of communications, but also potential conflicting interpretations and enforcement action from each individual supervisory authority;

b) Data controllers (or processors) with a "main establishment" in the pre-Brexit U.K. and one or more establishments in E.U. Member States: it is uncertain whether the ICO will continue to be the lead supervisory authority under the GDPR.[68] If not, then a U.K. establishment will no longer be capable of being a "main establishment" for the purposes of the GDPR or the one-stop-shop mechanism and, consequently, uncertainty would arise in respect of the criteria for ascertaining which (if any) of the E.U. establishments would become their "main establishment" for the purposes of the E.U. law. There will, of course, be cases where none of the E.U. establishments fall within the definition of "main establishment" under the GDPR and, in such cases, companies will fall outside the one-stop-shop mechanism; and

c) data controllers (or processors) established in the E.U. with no establishment in the U.K.: it is uncertain whether the ICO would be an additional supervisory authority,[69] whether the E.U. lead supervisory authority would continue to have sole jurisdiction if the ICO were to separately have jurisdiction, or what might be the level of cooperation between the ICO and the relevant supervisory authorities

[67] This is based on the assumption that no agreement is reached between the E.U. and the U.K. pursuant to which the ICO can continue as a supervisory authority capable of being a lead supervisory authority under the GDPR "one-stop shop mechanism".

[68] See paragraph 2.15 and subsequent above.

[69] As explained in paragraph 2.15 *ff.,* the E.U. Member State of the E.U. "main establishment" would be the lead supervisory authority and the other E.U. Member States where the organisation has establishments would be treated as "supervisory authorities concerned".

within the E.U. (both in terms of day-to-day dealings and in terms of business-critical enforcement actions), which could in turn strike a stark comparison with the objectives of cooperation and consistency so clearly set out under the GDPR.

3.15. In theory, upon Brexit, the U.K. will become a Third Country and not an E.U. Member State for the purposes of the GDPR cross-border consistency mechanism. Cooperation agreements between the E.U. and the U.K. would then fall into the international cooperation mechanisms and mutual assistance with Third Countries under Article 50 of the GDPR (see paragraph 2.20 above).

3.16. Nonetheless, HM Government has made it clear that it aims to achieve an enhanced role for the ICO alongside other European supervisory authorities after Brexit, in an attempt to ensure that effective dialogue and cooperation continue unhindered.[70] Given, however, that the exact nature of this cooperation remains to be seen, and given the recent commentary from the European Commission in this area,[71] there persists considerable uncertainty, especially in relation to enforcement action, where there could be potential for conflicting and/or inconsistent regulatory action being taken by E.U. supervisory authorities under the GDPR and the ICO. This might be unsettling.

3.17. How these uncertainties are resolved will likely tie to what, if anything, is agreed around the role of the ICO in the decision making processes of the EDPB. It is currently uncertain whether the E.U. will agree to the ICO retaining its seat on the EDPB, and it is reasonably foreseeable that the U.K. is prevented by Brexit from retaining its EDPB seat, leaving the U.K. as a Third Country with no official voice in European data protection regulation, while its businesses will still be subject to the full force of the GDPR through its extra-territorial effect.

Inconsistent interpretation by national supervisory authorities

3.18. Further to paragraphs 3.14 and subsequent above, potential inconsistencies in the implementation and enforcement of the data protection regime by the Data Protection

---

70 HM Government (Department for Exiting the European Union), "The exchange and protection of personal data (a future partnership paper)", 24 August 2017, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf.

71 In a "Notice to stakeholders on the withdrawal of the United Kingdom from the Union and E.U. rules in the field of data protection", it is stated that "In view of the considerable uncertainties, in particular concerning the content of a possible Withdrawal Agreement, all stakeholders processing personal data are reminded of legal repercussions, which need to be considered when the United Kingdom becomes a Third Country", available at: https://ec.europa.eu/info/law/law-topic/data-protection_en. See also the Commission's "Essential Principles" paper on the continued application of E.U. safeguards of personal data processed while the United Kingdom was a Member State, available at: https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

Supervisory Authorities of the E.U. Member States and/or the U.K. may give rise to legal uncertainties as to:

a) what "occasional processing" or "processing on a large scale" means for the purposes of the requirement to the designation of a representative in the E.U. (Article 27 GDPR), as well as for enforcement actions, which may therefore potentially be brought by more than one supervisory authority against a certain controller and/or processor (or their representatives within the E.U., if the case), which may cause different supervisory authorities to impose different fees to a certain controller or processor;

b) The requirement for controllers and processors without establishment in either the E.U. or the U.K. to designate a representative established in the E.U. and a representative established in the E.U., which in turn may cause penalties and fees to the controller and/or processor who has not designated a representative.[72] In fact, the DPA 2018 does not make clear whether controllers and processors established in the E.U. which do not have an establishment in the U.K. and offer services or goods to (or monitor the behaviour of) data subjects located in the U.K. will be required to designate a representative in the U.K. against which data subjects may bring claims. As noted above, the GDPR requirement for controllers and processors to appoint a representative in the E.U. is not replicated in the DPA 2018—i.e., it expressly excludes Article 27 of the GDPR and corresponding references to a "representative" from the "applied GDPR";[73] and

c) The nature and potential extent of a representative's liability for the non-compliance of the controller and/or processor that has designated it. Recital 80 and Article 27 of the GDPR provide that the designation of representatives shall not affect the responsibility/liability of the controller and/or processor, even in the case legal actions have been initiated against the controllers or processors themselves. Nevertheless, the designated representatives should be subject to enforcement in the event of the controller and/or processor's non-compliance

[72] On 22 July 2014, for instance, the Dutch DPA issued a compliance order against the instant messaging app WhatsApp as a result of its failure to designate a representative in the Netherlands, and imposed an administrative penalty of 10,000 EUR for each day that WhatsApp failed to comply. Please see: https://www.stibbe.com/en/news/2017/february/district-court-the-hague-whatsapp-is-more-than-data-transition-medium-and-must-appoint-dutch-repres ; and the case, in Dutch, is available at: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2016:14088

[73] The Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport (Lord Ashton of Hyde) has reaffirmed, during review of the Bill in the Committee stage in the House of Lords, that: "When the U.K. leaves the E.U., the powers in the E.U. withdrawal Bill will bring the GDPR into **our domestic law, anglicised**—as has been done to the applied GDPR—but also with other modifications that are dependent on the future negotiations with the EU." (Hansard, House of Lords Committee stage, 30 October 2017, Volume 785, Column 1207).

and, ultimately, in the event it is proved to be unfeasible or difficult to initiate legal actions against the controller or processor, it is conceivable the representative will be held liable. Also, it is unclear if enforcement action can be brought against DPOs appointed as defined in Section 69 of the DPA 2018, moreover because, though implied, there is no specific requirement for controllers and/or processors not established in the U.K. to appoint a DPO if their activities fall under the extra-territorial provisions of section 198 of the DPA 2018.

International cooperation and the jurisdiction/enforcement of data protection rights by U.K. data-subjects post-Brexit

3.19. On Brexit day, the U.K. will be a Third Country for the purposes of the GDPR, and, if there is no appointed representative present in the U.K., data subjects are likely to find the bringing of proceedings for infringements difficult. Post-Brexit, the enforcement of infringements under the DPA 2018 in the E.U. will be governed, as far as U.K. law is concerned, by section 120 of the DPA 2018 and will be a matter for international cooperation mechanisms rather than the mutual and reciprocal obligations of Member States.[74] It is uncertain, however, whether the European Commission will agree to mutual cooperation after Brexit and this gives rise to real and practical uncertainty.

3.20. Moreover, the GDPR does not *prima facie* offer any guarantee that, post-Brexit, data subjects located in the U.K. will be able to bring claims before the courts of:

a) an E.U. Member State for breaches of the GDPR, when, for example, the controller or processor is based in the E.U. and has no establishment in the U.K.;

b) an E.U. Member State for breaches of the U.K. Data Protection Regime which have extra-territorial effects;

c) The U.K. for breaches of the GDPR, where, for example, personal data of data subjects located in the U.K. is processed by an E.U. controller or processors with no establishment in the U.K.

3.21. Finally, it is still uncertain whether, post-Brexit, awards granted by U.K. courts will be recognised by and enforced in the E.U. in accordance with Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil

[74] Section 120 of DPA 2018 states that the ICO is to take appropriate steps to develop international cooperation. E.U. supervisory authorities must be willing to reciprocate, but at this stage, by no means is this certain.

and commercial matters (recast) (the "**Recast Brussels Regulation**"). This topic has been the subject of previous publications by the FMLC.[75]

The restriction on automated decision-making

3.22. Section 14 of DPA 2018 does not provide the authorisation referred to in Article 22(2)(b) of GDPR, which is, that the decision might be based solely on automated processing if authorised by the E.U. or the Member State law to which the controller is subject. Rather, it makes provision only in respect of the safeguards referred to in Article 22(2)(b). A controller must therefore look elsewhere for authorisation if it seeks to rely on this condition.

3.23. Both the guidance issued by the ICO on section 14 and the explanatory notes to the DPA 2018 make clear that the law in question does not need expressly to authorise decision-making which is wholly automated in order to fall within Article 22(2)(b). According to the explanatory notes, it is sufficient that the controller is subject to a legal obligation and that automated processing is a "reasonable way of complying with that requirement". This appears to give a controller some room for manoeuvre. Also implied in the explanatory notes, although not stated expressly, is the view that, for purposes of Article 22(2)(b) of the GDPR, the law providing the authorisation need not be the same as the law providing the safeguards (in the sense of, for example, arising under the same statute).

3.24. The ICO guidance is more stringent, stating instead that, "If you have a statutory or common law power to do something, and automated decision-making/profiling is the most appropriate way to achieve your purpose, then you may be able to justify this type of processing as authorised by law and rely on Article 22(2)(b). However, you must be able to show that it's reasonable to do so in all the circumstances."[76] This appears to be a significantly higher bar, and one subject to broader caveats, than suggested in the explanatory notes to the Act.

---

[75] See: FMLC, *"Issues of Legal Uncertainty Arising in the Context of the Withdrawal of the U.K. from the E.U.—The Application of English law, the Jurisdiction of English Courts and the Enforcement of English Judgments"* (December, 2016), available at: http://fmlc.org/report-u-k-withdrawal-from-the-e-u-2-december-2016/

[76] See link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/

4. IMPACT

4.1. As previously stated, the day-to-day operations of many businesses and organisations rely on the free movement of data to and from the U.K. under certain processing arrangements which will be significantly impacted with Brexit, as the U.K. becomes a Third Country.

4.2. The importance of cross border data flows cannot be underestimated: three quarters of the U.K.'s data transfers are with E.U. countries,[77] and many companies across the globe rely on personal data being sent to and from the U.K., including to and from data centres and data controllers and processors located in the U.K. With an ever-increasing use of cloud storage and Software-as-a-Service ("**SaaS**") applications, the day-to-day operations of many businesses and organisations rely on the free movement of data between the U.K. and the rest of the E.E.A., and current data processing arrangements generally prohibit or restrict data transfers outside the E.E.A.[78]

4.3. Furthermore, legal uncertainty in respect of the processing of personal data in the financial markets (in particular, by banking and insurance businesses) may undermine risk management, the adequate pricing of financial products,[79] operational continuity, and the prevention of fraud. It may also increase costs. For example, discrepancies in the interpretation or the application of legal concepts by each supervisory authority as they implement the data protection regime may result in different administrative penalties being imposed for the same act of non-compliance by different jurisdictions.[80] Likewise, uncertainties around the identity of the competent authority may result in a group, perhaps unnecessarily, setting up establishments in various jurisdictions (e.g.: set up a main establishment in the E.U. to benefit from the one-stop-shop mechanism). This will have particular relevance after Brexit, when there will be a potential for further divergences to emerge with time.

---

77 Please see the Frontier Economics independent report on "*The UK Digital Sectors after Brexit*", available at: https://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf.

78 The ICO notes that the GDPR restricts transfers of personal data outside the E.U., or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. See ICO guidance here on international transfers, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

79 As an example, these issues were extensively ventilated in the Second Reading of the Bill in the House of Lords.

80 For example, on 22 July 2014, the Dutch supervisory authority issued a compliance order against messaging app WhatsApp as a result of its failure to designate a representative in the Netherlands, and imposed an administrative penalty of EUR10,000.00 for each day that WhatsApp failed to comply.

4.4. All that is not to mention the data subject's enforcement rights, which might be compromised if legal uncertainties related to international cooperation and jurisdiction remain unresolved.

5. POTENTIAL SOLUTIONS AND MITIGANTS

5.1. In general terms, international cooperation mechanisms and transitional agreements between the U.K. and the E.U. could arguably clarify most of the issues of legal uncertainty identified above by expressly addressing them and clarifying the position. That is, however, dependent on Brexit negotiations and reciprocity and this is by no means certain unless and until an agreement is reached. Additionally, the following solutions and/or mitigants are proposed to address specific legal uncertainty issues.

The status of the U.K. post-Brexit—international transfers

5.2. As an alternative to the granting of an Adequacy Decision, the U.K. and the European Commission could consider an E.U.-U.K. Privacy Shield arrangement. Such an arrangement could be contemplated within the DPA 2018 for U.K.-certified organisations receiving personal data from the E.E.A. The European Commission will in any event need to make an Adequacy Decision that such an arrangement meets the adequacy requirements of Article 45(2) of the GDPR (as set out above in paragraphs 2.7 to 2.12), and time constraints may result in this kind of arrangement not being in place in time.

5.3. Alternatively, the U.K. could follow Adequacy Decisions made by the European Commission. In such cases, there would also need to be clear mechanisms and processes to adopt E.U. decisions made in response to validity challenges or as a result of regular reviews of Third Country compliance. These processes would need to specify whether decisions from the CJEU on such matters would be binding or whether there would need to be an additional legislative process in the U.K.

The E.U. consistency (or one-stop-shop) mechanism and the overlap of competence of U.K. and E.U. supervisory authorities post-Brexit

5.4. A transitional agreement alongside international cooperation might be an alternative to address such uncertainty, as to define the role of ICO in the decision making processes of the EDPB after Brexit, which in turn could help address uncertainty in relation to

enforcement and unsettling regulatory action from both E.U. and U.K. supervisory authorities.

Inconsistent interpretation by national supervisory authorities

5.5. With respect to the legal uncertainty arising out of the GDPR requirement for organisations established outside of the E.U. to designate, if certain conditions are met, a representative established in the E.U. vis-a-vis the lack of equivalent provisions in the DPA 2018 for organisations established outside the U.K. but offering goods or services to or monitoring the behaviour of U.K. data subjects after Brexit, a transitional arrangement, together with the equivalent U.K. legislation itself, could usefully clarify the position. The transitional arrangements and U.K. legislation could also clarify the extent of a representative's liability by setting out in more detail the circumstances in which it might arise and the parameters of any potential enforcement action against a representative.

Jurisdiction and enforcement of data protection rights by U.K. data-subjects post-Brexit

5.6. Mutual cooperation is essential to the cross-border enforcement of the rights of U.K. data-subjects under the GDPR as well as under the DPA 2018. Therefore mutual cooperation arrangements upon Brexit between the European Commission and the ICO may be of much assistance to address uncertainty in relation to the jurisdiction and enforcement of data protection rights by U.K. data-subjects post-Brexit. This issue would presumably need to be included in a transitional agreement.

The restriction on automated decision-making

5.7. In respect of the GDPR restriction on automated decision-making under Article 22 (see above, paragraph 2.22), ICO guidance apparently establishes a higher bar for compliance than the DPA 2018. The explanatory notes to the DPA 2018 suggest that it is sufficient that the controller is subject to a legal obligation and that automated decision-making/profiling is a reasonable way of complying with that legal requirement.[81] On the other hand, ICO guidance observes that even though there is a statutory or common law power to undertake automated decision-making/profiling, it must be reasonable to do so in all circumstances. This higher bar discrepancy between the ICO practice guidance and the DPA 2018 could usefully be clarified.

[81] See, in particular, note 115, available at: http://www.legislation.gov.uk/ukpga/2018/12/notes/division/6/index.htm

6. CONCLUSION

6.1. The objective of this paper has been to identify and, where appropriate, suggest potential solutions to issues of legal uncertainty which may arise in the context of the Data Protection Act 2018 alongside the GDPR. The FMLC has drawn attention, in particular to legal uncertainties related to:

a) International transfers of data in the context of Brexit and issues surrounding Adequacy Decision process and other modalities to transfer data lawfully to a Third Country, such as Model Clauses, which are under scrutiny of the CJEU;

b) Cross-border processing of data and the potential overlap of oversight competence between the U.K. and the E.U. supervisory authorities in the context of the consistency mechanism—the one stop shop mechanism;

c) Inconsistencies in the interpretation and enforcement of the Data Protection Regime by different supervisory authorities and the issue of the appointment of legal representatives and their liability;

d) Enforcement and jurisdiction of data protection rights of U.K. data-subjects after Brexit and the issue of the mutual international cooperation;

e) Potential overlap between the DPA 2018 and other laws, such as the LED, for the purposes of anti-money laundering and law enforcement; and

f) The restriction on automated decision-making in the GDPR, the DPA and ICO guidance.

6.2. Such uncertainties would have a significant impact on the financial markets as they have the potential to undermine risk management and operational continuity. Discrepancies between the interpretation and/or the application of legal concepts by each supervisory authority as they implement the data protection regime may result in different (potentially severe) administrative penalties being imposed for the same act of non-compliance by different jurisdictions. Likewise, uncertainties around identifying the competent authority may result in a group setting up establishments in various jurisdictions (e.g.: set up a main establishment in the E.U. to benefit from the one-stop-shop mechanism) with a consequential impact on overall efficiency. This will have

particular relevance after Brexit, when there will be potential for further divergences to emerge with time.

6.3. The data subject's enforcement rights may also be compromised if legal uncertainties related to international cooperation and jurisdiction remain unresolved.

6.4. To address these uncertainties, the FMLC has made recommendations for solutions and mitigants, as follows:

a) The settlement of an E.U.-U.K. Privacy Shield arrangement for UK-certified organisations receiving personal data from the E.E.A;

b) U.K. to follow Adequacy Decisions made by the European Commission, within a clear mechanism and process to adopt E.U. decisions;

c) A transitional agreement on:

i. international cooperation, to define the role of ICO in the decision making processes of the EDPB after Brexit and to define the jurisdiction and enforcement of data protection rights by U.K. data-subjects post-Brexit;

ii. interpretation of the requirement to appoint representatives, together with the equivalent U.K. legislation itself, could usefully clarify the position and the extent of their liability;

d) Further clarification from ICO, in consonance with the DPA 2018 in regard to the restriction on automated decision-making.

FINANCIAL MARKETS LAW COMMITTEE MEMBERS[82]

Lord Thomas of Cwmgiedd (Chairman)

David Greenwald (Deputy-Chairman)

Andrew Bagley, Goldman Sachs International

Sir William Blair, Queen Mary, University of London

Raymond Cox QC, Fountain Court Chambers

Hubert de Vauplane, Kramer Levin Naftalis & Frankel LLP

Michael Duncan, Allen & Overy LLP

Simon Firth, Linklaters LLP

Bradley J Gans, Citigroup

Kate Gibbons, Clifford Chance LLP

Richard Gray, HSBC Bank plc

Carolyn H. Jackson, Katten Muchin Rosenman U.K. LLP

Mark Kalderon, Freshfields Bruckhaus Deringer LLP

Rachel Kent, Hogan Lovells (International) LLP

Peter King, HM Treasury

Sir Robin Knowles CBE

Sean Martin, Financial Conduct Authority

Jon May, Marshall Wace LLP

Sinead Meany, Bank of England

Chris Newby, AIG

Jan Putnis, Slaughter and May

Barnabas Reynolds, Shearman & Sterling LLP

Peter Spires, Lloyd's of London

Sanjev Warna-kula-suriya, Latham & Watkins LLP

Pansy Wong, J.P. Morgan

Mr Justice Zacaroli

Joanna Perkins (Chief Executive)

[82] Note that Members act in a purely personal capacity. The names of the institutions that they ordinarily represent are given for information purposes only. Whilst the Bank of England, the Financial Conduct Authority and HM Treasury participate in the FMLC, the views expressed in this paper are not necessarily those of the three institutions.