OCTOBER 2014

FINANCIAL MARKETS LAW COMMITTEE

EU Data Protection Reform

Discussion of legal uncertainties arising in the area of EU Data Protection Reforms

www.fmlc.org

FINANCIAL MARKETS LAW COMMITTEE

WORKING GROUP[1]

Hannah Al-Rifai	AIG Europe Limited
Vivienne Artz	Citibank
Marcus Evans	Norton Rose Fulbright LLP
Kate Higginson	Financial Conduct Authority
Richard Jones	Clifford Chance LLP
Angela Teke	Association for Financial Markets in Europe
Joanna Perkins	FMLC Chief Executive
Sherine El-Sayed	FMLC Project Secretary
Paul Mortby	FMLC Issues 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.

CONTENTS

1. EXECUTIVE SUMMARY AND INTRODUCTION

Executive Summary

1.1 The role of the Financial Markets Law Committee (the "FMLC" or the "Committee") 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 This paper highlights issues of legal uncertainty which arise from the European Commission's Draft Regulation (the "Draft Regulation") and Directive (the "Draft Directive") on the protection of individuals with regard to the processing of personal data and on the free movement of such data (together the "Proposals").[2] The issues identified in this paper fall broadly into three categories: (i) definitional uncertainties; (ii) uncertainties arising from incompatibility with existing laws and regulation; and (iii) operational uncertainty likely to be caused when the Proposals take effect.

1.3 The FMLC previously commented on the Proposals in a letter to the EU Commission dated 8 July 2014.[3] In that letter, the FMLC drew attention to issues of legal uncertainty arising in the context of (i) data sharing agreements; (ii) the right to be forgotten; and (iii) the interaction with investigative powers in non-EU jurisdictions. Some of these issues are also addressed in this paper.

Introduction

1.4 The Proposals amend the existing regulatory approach introduced by Directive 95/46/EC, which was created to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. The current framework has not prevented fragmentation in the way the directive's provisions have been implemented across the EU and rapid technological developments have given rise to new challenges in the protection of personal data. The Proposals are therefore intended to address these issues by building a comprehensive and more coherent framework. The FMLC welcomes this but notes that, as currently drafted, the Proposals are likely to cause difficultly for data controllers and data processors which may have negative implications for the wholesale financial markets and also that they may restrict data-sharing between market participants and financial regulators, or

---

2 The proposal for a Regulation: COM(2012) 11 final; 2012/0011 (COD) and the proposal for a Directive: COM(2012) 10 final; 2012/0010 (COD).

3 FMLC letter to European Commission on "EU Data Protection Reforms" dated 8 July 2014: http://www.fmlc.org/uploads/2/6/5/8/26584807/eu_data_protection_reforms_letter_to_francoise_le_bail.pdf.

between financial regulators in different jurisdictions, which may have a negative impact on efforts to control financial crime.

1.5 Specifically, this paper addresses uncertainties arising from:

a. the interaction of the Draft Regulation and the Draft Directive;

b. incoherence in the internal structure of the Draft Regulation;

c. issues relating to the competence of authorities;

d. the Draft Regulation's approach to "main establishment"; and

e. the role, and responsibilities associated therewith, of "Data Protection Officers".

The paragraphs below examine these uncertainties in greater detail.

2. INCONSISTENCIES BETWEEN THE DRAFT DIRECTIVE AND REGULATION

2.1 The Proposals create two data processing regimes: (i) "general" processing, which is governed by the Draft Regulation; and (ii) processing for "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties", which is governed by the Draft Directive.[4] In accordance with Article 4 of the Draft Regulation and Article 3 of the Draft Directive, processing means any operation or set of operations performed on personal data including, *inter alia*, collection, recording, organisation, erasure or destruction.

2.2 In practice, it is not always possible to segregate general processing and criminal processing clearly and in this regard the Proposals give rise to uncertainty which may result in unworkable obligations for authorities that must process the same data for both criminal and administrative purposes.

2.3 The circumstances under which the processing of personal data falling within the scope of the Draft Directive is legitimate are set out in Article 7, which provides that processing is only lawful:

> *To the extent that processing is necessary:*
>
> *a) for the performance of a task carried out by a competent authority, based on law for the purposes set out in Article 1(1); or*
>
> *b) for compliance with a legal obligation to which the controller is subject; or*
>
> *c) in order to protect the vital interests of the data subject or of another person; or*
>
> *d) for the prevention of an immediate and serious threat to public security.*

2.4 According to these provisions, which are exhaustive, further or subsequent processing of data initially processed for the purposes of criminal investigation is not permissible. Recital 20, however, is framed in generally permissive terms as regards subsequent processing. It states: "personal data should not be processed for purposes incompatible with the purpose for which it was *collected*" (emphasis added). A similar approach is adopted in Article 4 of the Draft Directive (see, in particular, Article 4(b)). The interaction of Article 7 with these more permissive provisions is structurally

[4] Article 1 of the Draft Directive.

unclear. Given the restrictive tenor of Article 7, there is, therefore, considerable uncertainty as to the legality of any subsequent processing of personal data for matters unrelated to criminal offences where the data has initially been processed for the purposes relating to criminal investigation.

2.5 Logically, the processing of data for non-criminal purposes should fall within the ambit of the Regulation. There is, however, no provision made in the Proposals for the allocation of questions arising where data are collected for administrative purposes and are then subject to processing for both criminal investigatory and administrative purposes. One of the ways in which this lacuna could be addressed is by clarifying, under Article 7 of the Draft Directive, that processing which is not incompatible either with the purpose for which the data were collected or with processing in the context of criminal offences is lawful and is subject to the provisions of the Draft Regulation rather than the Draft Directive.

2.6 The application of the Proposals to data which may be the subject of both criminal investigatory and administrative (or other) processing is further obfuscated by the operation of Article 9(2)(j) of the Draft Regulation, which examines the processing of data with regard to criminal convictions, and Article 21(1)(b) of the Draft Regulation, which enables Member States to impose restrictions on the scope of certain key obligations and rights in order to safeguard the prevention, investigation, detection and prosecution of criminal offences. In conjunction with the provisions of the Draft Directive discussed above, these provisions create the possibility that data used for "criminal processing purposes" may be treated differently by different categories of user or indeed by the same category of user depending on whether processing takes place under the governance of the Draft Regulation or Directive. The FMLC recommends that further attention is given to the need for cohesion in the legal framework for data processing in cases where the same data are likely to be processed for both criminal and administrative purposes.

3. COMPETENT AND PUBLIC AUTHORITIES

3.1 The scope of the Draft Directive is limited to processing by "competent authorities", a term defined in Article 3 to mean

> *any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*.

This definition contemplates a broader range of authorities when compared with the ambit of the Framework Decision 2008/977 JHA, which it repeals. The wide scope gives rise to a lack of certainty regarding which entities should be considered as "competent" for the purpose of the Draft Directive. Arguably, any financial authority responsible for overseeing compliance with, for example, the Third Money Laundering Directive,[5] or competent for the purposes of the Market Abuse Directive,[6] will be categorised as "competent" under the Draft Directive owing to the authority's concern with the detection, investigation and prevention of activity that may also amount to a financial crime. It is not, however, clear that this is the intended result or that such administrative authorities regard themselves as competent in criminal matters. It is recommended that the definition of competent authorities in Article 3 is clarified in this respect.

3.2 Key provisions in the Draft Regulation exacerbate this uncertainty. Recital 16 refers to "public authorities" (as well as to "competent authorities") and states that data processed by such authorities under the Draft Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by a specific legal instrument, i.e. the Draft Directive. The term "public authorities" is not, however, defined in the Draft Regulation. Notwithstanding this lack of definition, the term appears twice: once in Article 4(19) where "supervisory authority" is defined as a public authority established by a Member State in accordance with Article 46; and also in Article 46 itself, which stipulates that a Member State shall provide that one or more public authorities are responsible for monitoring the application of the Regulation. The term "competent authority" is also left undefined in the Draft Regulation, although it appears in Article 2(2)(e), where processing "by competent authorities for the purposes of prevention… of criminal offences [etc]" is stipulated to be within the scope of the Draft Directive.[7] The FMLC recommends that Recital 16 and Article 2(2)(e) of the Draft Regulation are amended so that they are consistent with the scope of the Draft Directive and with one another.

---

5 Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

6 Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse).

7 The FMLC understands that new texts produced by both the Parliament and Council refer to "competent public authorities" but, as this term is also undefined, this amendment does not resolve the uncertainties addressed above.

4. COMPATABILITY WITH REGULATORY RULES AND INTERNATIONAL STANDARDS

4.1 The Draft Regulation outlines a list of derogations for which the processing of personal data may be deemed lawful (Article 6). In the absence of an applicable derogation, data processing will be unlawful if it contravenes any of the restrictions or obligations set out in the Draft Regulation or if it violates any of the rights which the Draft Regulation vests in the data subject, including the right to be forgotten (Article 17).

4.2 Article 6 includes a provision that data may be lawfully processed in order to comply with a "legal" obligation to which the controller may be subject under Article 6(1)(c). A similar approach is reflected in Article 17(3)(d) (concerning data retention) and Article 33(5) (concerning data protection impact assessments). The Draft Regulation does not, however, provide independently for the need to retain and process data for compliance with obligations which are purely regulatory.[8] It is true that Article 6(1)(e) and Recital 36 are slightly more permissive in that they contemplate processing "which is necessary for the performance of a task carried out in the public interest or in the exercise of official authority…" but it is not clear that retaining data to comply with regulatory requirements is "necessary for the performance of a task", other than the task of retention itself, or, on a narrow test, strictly "necessary… in the public interest".

4.3 This lacuna is particularly unfortunate in the context of the provision of financial services, where market participants are expected to comply with a particularly large and complex body of regulatory rules in carrying out their business activities. Two points are worthy of additional note:

1. in some EU jurisdictions, regulation may be classified as "law" but this is not true across all Member States; and

2. regulation encompasses a wide variety of normative techniques which may include any of the following: delegated legislation; non-legislative rule-

[8] It is, for example, unclear whether the processing and/or retention of information proposed to be required for the compiling of "insider lists" under Article 18(3) and (4) of Regulation (EU) No 596/2014 of 16 April 2014 on market abuse (the "Market Abuse Regulation") would fall within the Article 6 derogation under the Draft Regulation. Under current proposals, the information required to be included on an insider list includes, *inter alia*, the full name, home address, national identification number, telephone number(s) and email address(es) of the relevant person: paragraph 29.3 of the Draft Technical Standards on the Market Abuse Regulation published by the European Securities and Markets Authority on 15 July 2014.

making; orders; market guidance; individual guidance; and supervisory directions.

The FMLC would welcome further clarification that data processing in accordance with regulatory requirements and standards in any of the forms listed above will be compatible with the provisions of the Draft Regulation. In some cases, where domestic regulation implements, or specifies compliance with, international regulatory standards (for example those set by the International Organisation of Securities Commissions or the Financial Action Task Force) it would also be helpful to clarify that data processing in accordance with those standards is legitimate and compatible with the Draft Regulation.

4.4 For the avoidance of doubt and further uncertainty, the FMLC suggests that the Draft Regulation should be amended so that Article 6(1)(c) refers explicitly to "regulatory requirements". Alternatively, a definition should be inserted in Article 4 to clarify that "legal obligation" includes rules, guidelines, directions and orders made or given by competent regulatory authorities in Member States.

4.5 The FMLC does not comment on issues of policy. If, however, the Draft Regulation is intended to have the effect of prohibiting firms from complying with their regulatory requirements, whether within or outside of the EU, the FMLC considers that this would be a highly unusual legislative outcome.

5. INTERNAL COHERENCE OF THE DRAFT REGULATION

Definitional Issues

5.1 The Draft Regulation governs the processing of personal data which is wholly or partially intended to form a part of a filing system (Article 2(1)). For the purposes of Article 2, processing is any interaction with personal data, regardless of whether this is manual or by an automated process (Article 4(3)). It should also be noted that a processor is any entity which holds information for a controller (Article 4(6)). It is clear, therefore, that this sets a wide scope for the regulation of processing personal data. For example, the mere conversion of personal data from paper to an electronic format may constitute unlawful processing of personal data if it does not comply with the requirements of Article 6(1) of the Draft Regulation.

5.2 The FMLC would welcome guidance on the practical application of the wide definitions given to "processing" (Article 2) and "personal data" (Article 4).

5.3 The FMLC notes that Articles 5 and 6 incorporate a number of concepts or terms which are inherently vague. These include tests of fairness and transparency in Article 5(a) and a reference to the "vital interests" of the data subject in Article 6(1)(e). To the extent that the Draft Regulation relies on such concepts, which have a wide penumbra of conceptual uncertainty, it may be difficult for parties subject to its provisions (chiefly, the data subject and the data processor) to be clear about what they require.

Geographical Issues

5.4 The territorial scope of the Draft Regulation is laid down by Article 3:

> *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor of the Union.*
>
> *This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:*
>
> *a) the offering of goods or services in the Union; or*
>
> *b) the monitoring of their behaviour.*
>
> *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.*

5.5 According to this article, the territorial scope of the Draft Regulation is limited to processing by entities established in the Union and entities established in third countries who offer goods or services to data subjects within the Union, or who monitor the behaviour of data subjects in the Union.[9] The FMLC observes that, in the case of third country entities caught by the provisions of the Draft Regulation, the entities in question are likely to be subject to overlapping regulation, i.e. under their own home legal or regulatory system and under the Proposals. Evidently, this may lead to legal and/or regulatory conflicts. As a general principle, such regulatory conflict, exacerbated by the application of different standards and rules, causes significant legal uncertainties. Further details of the uncertainty which may be caused

[9] The FMLC notes that the most recent Parliamentary text, dated 12 March 2014: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402 of the Draft Regulation has emphasised and extended the extra-territorial effect of Article 3(1). Similarly the text removes the word "residing" from Article 3(2) requiring that a data subject is merely located "in the Union".

by regulatory conflict in third countries are set out in the FMLC letter dated 8 July (mentioned above). The FMLC would make two further and related points:

1. uncertainty as to the scope of the safe-harbours set out in Article 2(2),[10] in particular, uncertainty (discussed above) as to the definition of a "competent authority" in Article 2(2)(e) and any lack of clarity as to whether an activity is "exclusively" personal or not, are likely to exacerbate the difficulties caused by regulatory conflict; and

2. recent jurisprudence illustrates the risks associated with the storage of data in different geographical locations and legal jurisdictions.[11] Although it is not for the FMLC to comment on issues of policy, the Committee understands that financial market participants are concerned about the potential of the Draft Regulation to fragment the retention and storage of data along geographical and territorial lines to avoid the transfer of data into—or, indeed, out of—the Union and the likely increase in associated risks.

5.6 It was noted above that Article 6(1)(c) provides that processing may be legal where it "is necessary for compliance with a legal obligation to which the controller is subject". Paragraph 3 of that article stipulates that the legal obligation referred to must be one of Union law, or "the law of the Member State to which the controller is subject." This introduces a further issue of uncertainty in addition to those discussed above. First, there is uncertainty as to the boundaries of Union law. This gives rise to the question, for example, whether international conventions entered into by the EU, on behalf of its Member States, can impose a legal obligation. Second, there is the

---

[10] Article 2(2) provides that the Draft Regulation will

> *not apply to the processing of personal data:*
>
> *(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;*
>
> *(b) by the Union institutions, bodies, offices and agencies;*
>
> *(c) by the Members States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;*
>
> *(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;*
>
> *(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.*

[11] United States District Court Southern District of New York, *In the Matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft corporation*. 13 Mag. 2814.

practical question of the position of entities established in third countries that are required to process data to comply with obligations imposed by their "home" legal system and the confusion likely to be caused in these circumstances, where data processing is unlawful under the Regulation but obligatory in their home jurisdiction.

6. DATA PROCESSING IN THE ABSENCE OF CONSENT OR INSTRUCTION

6.1 The provisions of the Draft Regulation dealing with data subjects' rights to withdraw consent may cause further uncertainty. Article 6(1)(b) provides that processing is permitted where it is necessary for the purposes of the performance of a contract to which the data subject is a party. In practice, a contract which is to be performed by the data controller will stipulate that the data subject consents to data processing for the term of the contract. Contractual performance under Article 6(b) is, however, a separate ground of lawfulness from consent under Article 6(a). Uncertainty arises as a result of Article 7(3) which provides that the data subject shall have the right to withdraw his or her consent at any time: it is unclear whether contracts which prohibit the withdrawal of the data subject's consent during the term of the contract are compatible with Article 7(3). It is also unclear whether data processing remains lawful under either Article 6(a) or Article 6(b) when undertaken in performance of such a contract, if the data subject has breached the terms of the contract by purporting to withdraw his or her consent. The FMLC would be grateful for clarification that data processing under a contract with the data subject, where the data subject has given contractual consent to the processing during the life of the contract will not be characterised as unlawful merely because (i) the contract does not permit the data subject to withdraw his/her consent during the term of the contract; or (ii) the data subject purports to withdraw his/her consent in breach of contract.

6.2 It is not merely the withdrawal of consent which may create a situation in which data processing occurs outside the bounds of permission. Article 26(4) covers the situation where a processor exceeds the instructions it has been given by a data controller to process personal data. The article provides that, in these circumstances, the data processor is to be considered a data controller as regards any actions in excess of its instructions. It also makes the processor subject to the rules on joint controllers under Article 24. Article 24, however, does not provide for the development of a joint controller relationship by operation of the law in this way. Rather, it applies to situations where "a controller *determines* the purposes, conditions and means of

processing jointly with others" (emphasis added). This implies that the relationship is created expressly and cooperatively. It is very difficult to see how Article 24, which requires joint controllers to agree their respective responsibilities and an arrangement for the protection of the rights of the data subject, can apply in a situation which is, almost by definition, non-cooperative and contentious. The interaction between Articles 24 and 26 requires clarification.

7. PROCESSING AND THE RIGHT TO BE FORGOTTEN

7.1. Profiling is prohibited under the Draft Regulation and is defined under Article 20(1) as a measure which produces legal effects and

> *is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.*

Three exceptions to the prohibition of profiling are allowed under Article 20(2): (i) profiling carried out "in the course of the entering into, or performance of, a contract"; (ii) profiling "expressly authorized by a Union or Member State law"; and (iii) profiling "based on the data subject's consent".

7.2 Some businesses including typically insurance businesses, however, habitually utilise automated software applications and algorithms to characterise the market in which they operate and to determine an appropriate pricing strategy. It is not entirely clear whether this function would fall within the exemptions outlined in Article 20(2)(a) or (c).

7.3 Profiling activities may involve third, i.e. non-contracting, parties (one example from the retail insurance industry is the collection of data relating to other named drivers on a car insurance policy). This would fall within the scope of Article 20(1) and impinge upon the data subject's right not to be subject to certain types of profiling. By virtue of Article 20(2)(c), profiling is permitted if the data subject has given consent and the conditions for consent are outlined in Article 7 and referred to in Recital 33 of the Draft Regulation. These provisions raise the thresholds for consent by the criteria stipulated: Recital 33 requires a "genuine and free choice" to be made by the data subject and Article 7 provides that s/he must be able to withdraw consent at any time

without detriment. Uncertainty as to the operation of these provisions on consent where the data subject is also party to a contract with the data controller or processor is discussed above. However, the consent of data subjects who are not party to the contract and who are not bound to consent under its terms is likely to prove critical.

8. THE "ONE-STOP SHOP" AND MAIN ESTABLISHMENT

8.1 By virtue of Article 51(2), the supervisory authority of the "main establishment" of a data controller or data processor shall be competent for the supervision… of the controller or the processor in all Member States". This notion of a "home" supervisor for entities which operate in a cross-border environment is the first pillar of what has become known as "the One-Stop Shop ("OSS") mechanism" for the supervision of entities subject to the Draft Regulation. It represents an intention to introduce a consistent and coordinated supervisory approach to data processing by organisations that carry on business in multiple EU Member States. The intended outcome appears to be that a single Member State's Supervisory Authority will be competent to supervise the controller or processor's activities with the assistance and oversight of supervisory authorities in other relevant states. There is considerable uncertainty, however, as to whether the provisions of the Draft Regulation will be effective to achieve that objective.

8.2 The interaction of Article 51(2) with the definition of a data controller, which includes any "*legal person*…which… determines the purposes, conditions and means of the processing of personal data" (emphasis added), in the case of groups of undertakings operating in a cross-border environment is unclear because, according to the definition, individual undertakings within a group are each capable, *qua* legal person, of being identified as a data controller whereas the concept of a "main establishment", which appears in Article 50(2)(f) of the Treaty of the Functioning of the European Union ("TFEU"),[12] can refer equally to the parent of subsidiaries or the company headquarters of satellite branches. In the TFEU the concept of a "main establishment" is ancillary to the fundamental treaty principle of freedom of establishment and it is unnecessary, therefore, to distinguish between an undertaking's intention to establish itself in Member States by means of subsidiaries or by means of branches. In contrast, the supervisory schema contemplated by the Draft Regulation, requires the identification of a "main establishment" for each "legal person" who is a

[12] consolidated version C 326/50 of 2012.

data controller and, by that means, a lead supervisor. It is important in this context, to ascertain whether, where an undertaking is established by means of subsidiaries all of whom are engaged to some degree in determining, say, the means of processing data, the concepts of "main establishment" and "data controller" are to be identified as one legal person for the group as a whole or additionally for each legal person in the group who is engaged in determining various aspects of data processing, particularly in the case of those subsidiaries who themselves operate through branches.

8.3 A second pillar of the proposed OSS mechanism is the provision for "binding corporate rules", which is one of the means by which data may legitimately be transferred within a corporate group to a third country (see Articles 42 and 43) in cases where the EU Commission has not reached an adequacy decision in respect of that third country under Article 41. Binding corporate rules designed to provide the data subject with adequate protection in the event of a data transfer are to be approved for a group of undertakings by the competent supervisory authority identified under Article 51. A "group of undertakings" is defined in Article 4 as "a controlling undertaking and its controlled undertakings" (where "controlling" and "controlled" are unrelated to the concept of a data "controller"). It is not clear how this idea of a highly centralised group is intended to interact with the first pillar of the OSS mechanism, i.e. supervisory competence based on the "main establishment" of a data controller), given some uncertainty, noted above, as to whether a group may comprise a single or multiple data controller(s).

8.4 The proposed OSS mechanism relies on three additional elements. First, the concept of a main establishment of data controllers and processors, intended to determine which is the lead supervisory authority. Secondly, provision for mutual assistance and increased cooperation between supervisory authorities. Thirdly, a consistency mechanism is introduced under Article 57 which is designed to ensure common interpretation and enforcement of the Draft Regulation across the EU. The FMLC has identified further issues of legal uncertainty in respect of the first two elements.

Main Establishment

8.5 Under Article 4(13) of the Draft Regulation a controller's main establishment is determined by the location where key decisions are taken, affecting the "purposes, conditions and means" by which data are processed. Should decisions be taken outside the EU, the controller's main establishment will be where the "main processing activities take place" within the EU. On the other hand, "[a]s regards the

processor, 'main establishment' means the place of its central administration in the Union".

8.6 The FMLC considers that these definitions do not fully take into account the intricacies of large EU group entities and the legal and regulatory regimes which already affect the ways in which they may retain, process and control data. The approach in Article 51 would not appear to accommodate situations which fall outside the circumstances of either single legal entities with multiple branches across the EU or groups of separate entities which have at their centre a data controller which clearly governs the others as data processors. In some cases it may simply be unclear, as discussed above, whether a group containing several subsidiaries has one or more data controllers. In other cases, groups of undertakings may be unwilling or unable to surrender to a single group company the control of data processing owing to the imposition of regulatory rules which require group companies to operate at arm's length in the processing of market sensitive data and in determining how that data is processed. For example, hypothetically-speaking, a group in which the various regional subsidiaries published benchmarks compiled from personal financial data would not be in a position to designate one company as data controller for the group in the event that those benchmarks were individually to become subject to national regulation.

8.7 The FMLC understands that recent amendments proposed by the EU Parliament and Council have attempted to address some of the difficulties discussed above by introducing requirements for controllers to collate and submit information on countries of establishment and activity and the means of processing to supervisory authorities for verification and further submission to the European Data Protection Board which, in turn, will maintain a public register of this information.[13] Such a requirement would reduce uncertainty as to the identification of the lead supervisory authority and would be welcomed by the FMLC.

Competency of Supervisory Authorities

8.8 Although Article 51(2) provides a mechanism for identifying the competent authority for the purposes of supervision, it is not clear from the text whether the competence thus conferred on the lead supervisor is exclusive or not. The Draft Regulation's

[13] Parliament's position paper dated 12 March 2014: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402 and the Council's position paper dated 30 April 2014: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209327%202014%20INIT.

provision for mutual assistance and cooperation between supervisors suggests, perhaps, that competence is non-exclusive. The FMLC understands that this issue has been raised for co-decision and addressed in recent amendments to the text. It would welcome further clarification on the question of supervisory competence.

9. DATA PROTECTION OFFICERS

9.1 The Draft Regulation outlines specific circumstances under which a data protection officer should be appointed by the controller and processor and Article 35(2) provides for the appointment of a single data protection officer in the case of group undertakings. The controller and processor must ensure that data protection officers are appointed

> *on the basis of professional qualities, in particular, expert knowledge of data protection law and practice and the ability to fulfil tasks referred to in Article 37 […]*

Uncertainty arises with regard to the precise nature and scope of legal expertise that a data protection officer must possess. It is not clear, for example, whether a data protection officer is required to have expert knowledge of local data protection laws and practices in each of the jurisdictions over which he or she is to have oversight. Operational uncertainty is likely to arise for large organisations or firms operating in multiple Member States if comprehensive expertise is required, owing to the difficulty in hiring individuals with sufficient expertise across all the jurisdictions in which the organisation operates. The FMLC would welcome greater clarity.

10. CONCLUSION

10.1 The objective of this paper has been to identify and, where appropriate, suggest potential solutions or improvements to issues of legal uncertainty affecting the wholesale financial markets arising from the Draft Regulation and Draft Directive. The FMLC has drawn attention to issues of uncertainty arising from, in particular, (i) the interplay between the Draft Regulation and Draft Directive; (ii) internal incoherence in the Draft Regulation; (iii) the provisions on competent authorities; and (iv) the OSS mechanism and the term "main establishment". To address these uncertainties, this paper sets out a number of proposed solutions which include,

among other things, that further (i) attention is given to the need for cohesion in the legal framework of data processing cases; (ii) clarification is given to specific definitions and concepts set out in the Proposals; and (iii) guidance is provided with regards to certain provisions in the Proposals.

FINANCIAL MARKETS LAW COMMITTEE MEMBERS*

Lord Walker (Chairman)

David Greenwald (Deputy-Chairman)

Andrew Bagley, Goldman Sachs International

Charles Barter, Bridgepoint

Sir William Blair

Hubert de Vauplane, Kramer Levin Naftalis & Frankel LLP

Simon Dodds, Deutsche Bank AG

Michael Duncan, Allen & Overy LLP

Simon Firth, Linklaters LLP

Bradley J Gans, Citigroup

Kate Gibbons, Clifford Chance LLP

Richard Gray, HSBC Bank plc

Wim Hautekiet, Bank of New York Mellon SA/NV

Mark Kalderon, Freshfields Bruckhaus Deringer LLP

Sir Robin Knowles CBE

Piers Le Marchant, JPMorgan Chase Bank, N.A.

Sean Martin, Financial Conduct Authority

Jon May, Marshall Wace LLP

Sean McGovern, Lloyd's of London

Chris Newby, AIG

Graham Nicholson, Bank of England

Stephen Parker, HM Treasury

Sanjev Warna-kula-suriya, Slaughter and May

Geoffrey Yeowart, Hogan Lovells International LLP

Chief Executive: Joanna Perkins

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