Report on innovative uses of consumer data by financial institutions

28 June 2017

EBA EUROPEAN BANKING AUTHORITY

Contents

Abbreviations

A29WP	Article 29 Data Protection Working Party
AIS	Account information services
AML/CFT	Anti-money laundering/ countering the financing of terrorism
AMLD	Anti-Money Laundering Directive
DP	Discussion Paper
DPA	Data protection authority
DPIA	Data Protection Impact Assessment
DPO	Data protection officer
EBA	European Banking Authority
EDPS	European Data Protection Supervisor
EIOPA	European Insurance and Occupational Pensions Authority
ESAs	European Supervisory Authorities (the EBA, ESMA and EIOPA)
ESMA	European Securities and Markets Authority
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and communication technology
JC	Joint Committee
MCD	Mortgage Credit Directive
NIS Directive	Security of Network and Information Systems Directive
PAD	Payments Account Directive
PIS	Payment initiation services
PSD1	Payment Services Directive (2007/63/EC)
PSD2	Revised Payment Services Directive (2015/2366)
PSPs	Payment service providers
RTS	Regulatory Technical Standards
TPPs	Third-party payment providers
UCPD	Unfair Commercial Practices Directive

Executive summary

Article 9(4) of the EBA's founding Regulation mandates the EBA to monitor financial innovation across the European Union (EU) and to foster a consistent supervisory approach to these innovations. In this context, the EBA observed that a growing number of financial institutions use consumer data in innovative ways, often combining data that they hold internally with data obtained from external data vendors or social media.

Following a preliminary analysis of this particular innovation, the EBA published, on 4 May 2016, a Discussion Paper (DP) that presented the risks and potential benefits of this particular innovation identified by the EBA and asked market participants to comment on whether the EBA's analysis fairly reflected current market practices.

After assessing the responses and examining the applicability of the EU legal provisions currently in force on the management and utilisation of consumer data by financial institutions, the EBA reached six conclusions.

First, although the innovative uses of data identified in the DP are not equally widespread throughout the EU, the proliferation of the innovation is accelerating, and therefore deserves ongoing monitoring by supervisory authorities. A number of factors are expected to contribute to a further acceleration of this innovation, including the revised Payment Services Directive (PSD2), the new data portability requirements under the General Data Protection Regulation (GDPR) and the development of new technological innovations such as Big Data analytics, artificial intelligence and robo-advice.

Second, the risks identified by the EBA were fairly presented in the DP, although the likelihood of their materialisation might vary. Third, provided that the risks identified are mitigated, innovative uses of data can have potential benefits for consumers, through enhanced product quality and services better tailored to their needs. Financial institutions, in turn, might benefit from enhanced cost/revenue efficiency, better risk management and regulatory compliance.

Fourth, the use of consumer data is already subject to an extensive set of legal requirements, some of which, such as the GDPR and PSD2 have not been yet fully applied across the EU. In particular, the GDPR, which will apply from 25 May 2018, is one of the key pieces of legislation that will provide a comprehensive legal framework on the processing of personal data, applicable to all providers that process personal data of EU individuals. Its requirements on transparency, automatic profiling, data minimisation, purpose limitation, accuracy, confidentiality and accountability, alongside the additional requirements deriving from other EU legislative acts that financial institutions are required to abide by, such as the PSD2, the Payment Account Directive, the Mortgage Credit Directive, the Anti-Money Laundering Directive and the Unfair Commercial Practices Directive, mitigate, to different extents, many of the risks identified by the EBA.

Fifth, the risks arising specifically from Big Data analytics are cross-sectoral and will therefore be further assessed in forthcoming joint work with ESMA and EIOPA.

Sixth, after assessing the applicability of existing EU law to this particular innovation, the EBA finds no sufficient grounds for further industry-specific legislative interventions at this point in time, but will continue to monitor closely the evolution of this innovation, including through concrete case studies, and engage in further cooperation with the other ESAs, the European Commission and EU data protection supervisors. The EBA also encourages cooperation between national competent authorities across all relevant policy areas, in order to ensure that the legal requirements on the use of data are applied consistently across the 28 Member States, and encourages further education initiatives to raise consumer awareness on this topic.

Background

1. On 4 May 2016, the EBA published a DP on innovative uses of consumer data by financial institutions[1]. In fulfilment of its task to monitor financial innovation as set out in Article 9(4) of its founding Regulation[2], the EBA has observed a growing number of financial institutions using consumer data in innovative ways across the EBA's regulatory remit, comprising deposits, mortgages, personal loans, payment accounts, payment services and electronic money[3].

2. The DP identified a number of practices that the EBA has observed in the market, such as financial institutions using data that they hold internally, often combined with data obtained from external sources, including data vendors or social media, to provide tailor-made offers to consumers, for credit scoring or early detection of customers' default risk, or to offer shopping discounts from other companies based on consumers' existing payment data and spending behaviour.

3. The DP also highlighted a number of potential benefits and risks associated with this particular innovation, as well as some of the legal requirements that already apply to the phenomenon. The DP was aimed at receiving input from market participants on whether the innovative uses of consumer data that the EBA has identified are comprehensive and reflect current practices, and whether the risks and potential benefits were fairly reflected, in order to allow the EBA to make a better informed decision on what regulatory and/or supervisory response, if any, the EBA should take or propose.

4. In the DP, the EBA acknowledged that, among other types of consumer data, the use of payment data in the market segment of retail payments is of particular interest to the EBA because, unlike other, one-off, types of data provided by consumers, payments data provide financial institutions with a continuous and extensive insight into consumers' purchasing habits, preferences and, therefore, lifestyle more generally.

5. Following a three-month consultation period, the EBA received 35 responses to the DP, of which 6 were confidential. Thirteen responses were received from trade associations, seven from financial institutions, six from consumer associations, one from the EBA's Banking Stakeholder Group and eight from other categories of respondents.

6. After assessing those responses and examining the applicability of the EU legal provisions in force on the management and utilisation of consumer data by financial institutions, the EBA reached six conclusions, as outlined below.

[1] Available here
[2] Regulation (EU) No 1093/2010
[3] For the purposes of this report, the term 'financial institutions' refers to financial institutions that fall within the EBA's remit, comprising credit institutions, creditors, credit intermediaries, payment institutions and e-money institutions. Also for the purposes of this report, the use of consumer data encompasses the collection, processing and storage of data, including the use of aggregation tools and other data processing technologies.

Conclusions

A. Although the innovative uses of data identified in the DP are not equally widespread throughout the EU, the use of consumer data is accelerating

7. From the analysis of responses to the DP, financial institutions seem to be increasingly using consumer data in innovative ways, although not all of the innovations identified in the DP are equally widespread throughout the EU.

8. For example, a number of respondents, in particular from the banking sector, specifically pointed out that the use of social media data by banks has until now been limited by the legal uncertainty surrounding the use of this kind of data and because of potential customers' distrust, although some banks are investigating the use of such data as a potential complementary source of information. A few respondents also referred to financial institutions selling customers' data to third parties, but did not offer concrete examples or evidence to support those claims. The EBA will further assess the development of these practices based on additional sources of information, as part of its ongoing monitoring of the phenomenon.

9. Respondents generally emphasised that the use of consumer data very much depends on a number of factors, such as the type of financial institution, the product in question and the data available from credit bureaus. For instance, in some countries only 'negative' data, such as defaults on a previous loan, are available to banks, whereas in other countries 'positive' data, such as other current loans and similar financial commitments, are also available.

10. Some respondents emphasised that there is an imbalance between financial institutions that gather/hold a large number of consumer data (such as payment/transaction data) and new market entrants. They were of the view that 'traditional' retail banks use fewer external sources of data than internal sources, whereas other players in the market, such as FinTech companies[4] and big digital players, can often resort to a greater variety of data about users either collected directly via their services or via access to other forms of data such as social networking, online behaviour etc.[5].

11. The most common uses of consumer data mentioned by respondents were related to marketing, consumer profiling and segmentation, legal compliance (e.g., anti-money laundering/countering the financing of terrorism (AML/CFT)), risk management and developing personalised offers.

[4] For the purpose of this report and in line with the definition used by the Financial Stability Board (FSB), FinTech means 'technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services' (FSB, Standing Committee on Assessment of Vulnerabilities, 'FinTech: Describing the Landscape and Framework for Analysis', 16 March 2016).

[5] For instance, a few respondents referred to some FinTech companies that have developed online lending models based on an analysis of social networking data.

12. However, respondents generally agreed that innovative uses of data are increasing, as financial and non-financial companies collect more and more consumer data in an attempt to predict, with a higher level of accuracy, consumers' preferences, future behaviour and risk profile.

13. New regulatory developments, such as the revised Payment Services Directive (PSD2), which will apply from 13 January 2018 and will give new third party providers access to payment account data held by banks, or the new right to data portability under the GDPR[6], are expected to contribute to an increase in innovative uses of data and foster competition in offering new innovative services. This, coupled with the continuing increase in computing power and storage capacity, and in the use of data analytics-methods to interpret vast quantities of data, or 'Big Data'[7], as well as the development of other FinTech innovations, such as artificial intelligence, robo-advice, the internet of things, the use of technological innovations for compliance purposes (or 'RegTech') and the development of 'open-banking' standards, may further foster innovative uses of data and potentially change the way in which the market will evolve in the future.

B. The risks identified by the EBA were fairly presented in the DP, although the likelihood and impact of their materialisation might vary

14. In the DP, the EBA identified several risks of innovative uses of consumer data, such as:

- the risk that consumers will not be properly informed of, or not be able to understand, how their data are being used;
- the risk that consumers' data will be misused for purposes that were not disclosed to them, or to which they did not consent;
- the risk that decisions will be taken based on inaccurate information;
- the risk that consumers' ability to change providers will be restricted if financial institutions do not allow them to transfer their data to a new provider ('lock-in' risk);
- security and cybersecurity risks;
- reputational risks to financial institutions if they make questionable use of consumer data; and
- risks related to the integrity of the financial sector as a result of security incidents or financial institutions becoming overly dependent on the use of consumer data.

[6] 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

[7] The term 'Big Data' is generally used to refer to large volumes of different types of data, produced with high velocity from many and varied sources (such as the internet of things, sensors, social media, financial markets data, etc.), which are processed, often in real time, by IT tools (powerful processors, software and algorithms). See also the Discussion Paper on the use of Big Data by financial institutions, published by Joint Committee (JC) of the three ESAs on 19 December 2016.

15. Respondents generally agreed with the risks identified in the DP, although many were of the view that most of these risks are not confined to the innovative use of consumer data by financial institutions, but, rather, are business risks common to other business areas, and that the likelihood and impact of the materialisation of those risks might vary.

16. For example, while many respondents, particularly from the financial sector, were of the view that the existing legislation already mitigates most of the risks identified in the DP, respondents generally perceive cybersecurity as a real concern, particularly in the context of an increasing interconnectedness within the financial sector and of the PSD2 giving new entrants to the market access to payment account data.

17. Financial institutions also raised concerns regarding a potential lack of a level playing field between banks and the new entrants to the market, such as FinTech start-ups or large digital players, although few of them offer concrete examples of an unlevel playing field. The EBA notes that most of the concerns expressed on this topic by respondents, particularly from the banking sector, relate to the policy choices made by EU legislators under the PSD2 that require banks to open up access to payment account data to new third-party providers. In addition, a few respondents were of the view that any company holding customers' financial data should be brought under the perimeter of the Security of Network and Information Systems Directive (NIS Directive)[8], and that this should not be the case only for credit institutions that are identified as 'operators of essential services'.

18. Having assessed the responses, the EBA considers that the risks identified in the DP were fairly summarised, although not all are specific to this innovation and the likelihood of their materialisation might vary[9].

C. Provided that the risks identified are mitigated, innovative uses of data can have potential benefits for consumers and financial institutions

19. The potential benefits identified by the EBA in the DP resonated well with many respondents, although consumer associations were generally more sceptical about potential benefits for consumers. Consumer associations were particularly concerned that data could be mis-used to target vulnerable consumers, regarding non-transparent dynamic pricing techniques or that personalised offers could encourage frivolous spending or hyper-consumerism, and expressed doubts that reductions in costs achieved by financial institutions would be passed on to consumers.

20. Some respondents were of the view that innovative uses of data may support financial inclusion by increasing the accessibility of financial products to consumers, especially for borrowers who do not generally have access to credit because of limited credit information data, although this remains questionable in the absence of evidence. On the other hand,

[8] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

[9] Additional specific risks that respondents have highlighted concerning the use of Big Data analytics are outlined in section E below.

other respondents, particularly consumer associations, were not convinced that extensive use of customer data can increase the accuracy of creditworthiness assessments, or make the credit affordable to a larger number of customers, and argued that extensive use of customer data may lead to financial exclusion. EU consumer associations were of the opinion that the information that 'can be found on the consumer's bank/payment account statement', covering a sufficiently long period of time, is fully sufficient by itself to assess the creditworthiness of the customer.

21. Both consumer associations and the representatives of the financial service providers generally agreed that using customer data may contribute to better protection against fraud. Some consumer associations were of the view that using consumer data to improve fraud detection and offering consumers better insight into their financial situation and advice in financial services are the most important benefits to consumers, provided that algorithms are designed well. Furthermore, both consumer associations and industry representatives agreed that, in addition to the potential benefits to consumers outlined in the DP, transaction speed can be greatly increased for consumers.

22. Overall, the EBA considers that, if risks are mitigated, innovative uses of data may have benefits for consumers by enhancing product quality and offering them more tailored services adapted to their needs and a better insight into their financial situation. They might also lead to cost savings for consumers, although not necessarily through cost savings on marketing campaigns achieved by financial institutions being passed on to consumers, which remains questionable, but for example through offering consumers targeted discounts with specific trading partners. In turn, financial institutions may also benefit from enhanced cost/revenue efficiency, better risk management and regulatory compliance.

D. The use of consumer data is already subject to an extensive set of legal requirements, which financial institutions must comply with, and which mitigate, to different extents, most of the risks identified by the EBA

23. Feedback received from the public consultation suggests that many respondents, particularly from the financial sector, consider that the existing legal requirements provide sufficient mitigation against the risks identified and that there is no need for additional industry-specific rules in the financial sector. Respondents also stressed that newly introduced legislation in this area specific to financial institutions may aggravate the risks of an unlevel playing field with other, non-financial providers that may be subject to less extensive regulatory requirements.

24. In order for the EBA to make its own assessment of the extent to which the specific risks identified may already be mitigated by existing legislation, the EBA reviewed a number of EU regulations and directives, such as the GDPR, the PSD2, the Payment Account Directive

(PAD)[10], the Mortgage Credit Directive (MCD)[11], the fourth Anti-Money Laundering Directive (AMLD)[12] and the Unfair Commercial Practices Directive (UCPD)[13]. This section provides a brief summary of some of the legal requirements that may apply to this innovation, but is not intended to be exhaustive and conclusive.

25. The GDPR, which will apply from 25 May 2018[14], is one of the key pieces of legislation that is particularly relevant for this topic and aims to address many of the risks outlined in the DP (e.g. regarding misuse/non-disclosed use of data, and data portability). The principles of data protection under the GDPR will apply to 'any information concerning an identified or identifiable natural person', be it publicly available or not. As noted by the Article 29 Data Protection Working Party (A29WP), 'the mere fact that such data has been made publicly available does not lead to an exemption from data protection law', including, as detailed below, the requirements under the GDPR that need to be met in order for firms to be able to reuse such data for other purposes[15].

26. As regards the risks identified in the DP relating to information asymmetries, the GDPR aims to address these risks by requiring that the processing of personal data is fair and transparent (Article 5(1)(a) of the GDPR). This means, among other things, that individuals must be informed, 'in clear and plain language', about the purposes for which their personal data are collected and processed and with whom their personal data are shared, including whether data obtained from other sources (such as social network data) will be used (see Articles 13 and 14 of the GDPR).

27. Other provisions under the GDPR further aim to put consumers in greater control of their personal data, for example by giving them the right to access the personal data collected about them (Article 15), to obtain the rectification of inaccurate personal data (Article 16), to obtain the erasure of their personal data, for example where it is no longer necessary for the purposes for which it was collected (Article 17), and the right to object to the processing, for example where data is used for direct marketing purposes (Article 21).

28. Moreover, under the GDPR, any processing of personal data must be based on a legal basis, as set out in Article 6 of the GDPR, consent being one such potential legal basis. Where the processing is based on consent, the GDPR introduces more stringent requirements for consent to be considered as validly given, by requiring that consent should be 'freely given, specific, informed and unambiguous' and expressed 'by a statement or by a clear affirmative action' (Articles 4(11) and 7 and Recitals 32, 42 and 43 of the GDPR). Additional restrictions apply to the processing of certain categories of data deemed 'sensitive data', which include health data and biometric data (Article 9).

29. In addition, a key principle under the GDPR, that may impact on firms' capacity to have recourse to extensive sources of data, is that personal data shall be 'adequate, relevant and

[10] Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features
[11] Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property
[12] Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
[13] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market
[14] The GDPR will, from 25 May 2018, replace the current Data Protection Directive (Directive 95/46/EC).
[15] A29WP Opinion on Purpose Limitation, published on 2 April 2013, p. 35.

limited to what is necessary in relation to the purpose for which they are processed' ('data minimisation' principle) and shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed' ('storage limitation' principle) (Article 5(1) (c) and (d) of the GDPR).

30. The risk of consumers' data being misused for other purposes is further mitigated by the requirements under the GDPR that personal data can be collected only for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' ('purpose limitation' principle) (Article 5 (1)(b)). As noted by the European Data Protection Supervisor (EDPS), 'further processing for a secondary purpose is not forbidden, but the secondary purpose must not be "incompatible" with the purposes for which the data have been collected'[16].

31. The A29WP's Opinion on Purpose Limitation from 2013 specifically assesses the application of this principle to Big Data and takes the view that, where Big Data analytics is used to analyse or predict the personal preferences, behaviour and attitudes of individual customers, in order to inform measures or decisions that are taken with regard to those customers, 'consent would almost always be required, otherwise further use cannot be considered compatible'. The A29WP's Opinion further adds that: 'For the consent to be informed, and to ensure transparency, data subjects/consumers should be given access to their "profiles", as well as to the logic of the decision-making (algorithm) that led to the development of the profile. In other words: organisations should disclose their decisional criteria. […] Further, the source of the data that led to the creation of the profile should also be disclosed'[17].

32. This principle of purpose limitation is also reflected in the fourth AMLD, of which Article 41 prohibits the further processing of data collected for AML/CFT purposes, for incompatible purposes and in particular for commercial purposes.

33. In the payment services sector, the PSD2 reaffirms the application of the 'principles of necessity, proportionality, purpose limitation and proportionate data retention period' under the data protection legislation to payment service providers (PSPs) (Recital 89 of the PSD2). Furthermore, in line with the data minimisation principle stated above, Article 94(2) of the PSD2 provides that PSPs 'shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user'.

34. In addition to this general principle, the PSD2 also sets out a series of specific safeguards applicable to the new third-party payment providers (TPPs) offering account information services (AIS) and payment initiation services (PIS) when accessing customers' data, and specifically prohibits these providers from using, accessing or storing any data for purposes other than for performing the account information or, respectively, the payment initiation service explicitly requested by the customer (Articles 66 and 67 of the PSD2).

[16] EDPS Preliminary Opinion on 'Privacy and Competitiveness in the Age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy', published in 26 March 2014, p. 14.
[17] A29WP Opinion on Purpose Limitation, published on 2 April 2013, p. 47. See also the Statement of the A29WP on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU, published on 16 September 2014.

35. Furthermore, the GDPR promotes accountability and governance measures. One of the most important novelties introduced by the GDPR is the principle of accountability, according to which firms are expected to be able to demonstrate that they have taken the necessary steps to ensure compliance with the GDPR. This has a number of implications, and many firms will be required to:

    - appoint a data protection officer (DPO) (Articles 37 - 39);
    - adopt internal policies and implement measures that meet the principles of data protection by design and by default (Article 25 and Recital 78);
    - undertake data protection impact assessments (DPIA)(Article 35); and
    - voluntarily join and adhere to approved codes of conduct or approved certification mechanisms, which may be used as an element by which to demonstrate compliance with the GDPR (Articles 24(3), 28(5) and 40-43 of the GDPR).

36. Under the GDPR, certain firms will be required to appoint a DPO, for example if they engage, as a core activity, in monitoring individuals systematically and on a large scale, or if they process special categories of personal data on a large scale (Article 37). The GDPR provides certain safeguards to ensure that DPOs are given sufficient autonomy and resources to carry out their tasks effectively, and specifies, for example, that DPOs must have a direct reporting line 'to the highest management level' of the company (Articles 38 and 39 of the GDPR)[18].

37. Furthermore, the GDPR requires that a DPIA is carried out, before the start of the processing, where a type of processing is 'likely to result in a high risk to the rights and freedoms of natural persons' (Article 35(1)). For example, certain profiling activities, Big Data projects or the introduction of new data processing technologies may trigger the need to carry out a DPIA. The Guidelines issued by the A29WP provide further guidance on when a DPIA is required and provide criteria that data protection authorities (DPAs) may use to establish the lists of processing operations that will be subject to the DPIA requirement[19].

38. Where the outcome of a DPIA indicates a level of data protection risk that firms feel they cannot address with their own (reasonable) means, they should liaise with the relevant DPA, in order to discuss alternative, more effective measures (Recital 94 and Article 36 of the GDPR).

39. In addition, the rules in the GDPR regarding the transfer of personal data to locations outside the European Economic Area (EEA) should be considered where data are shared among different entities across jurisdictions.

40. As regards the risk mentioned in the DP relating to decisions being taken on the basis of outdated or inaccurate information, various legal requirements aim to mitigate, to some extent, this risk. For example, Article 5(1)(d) of the GDPR requires that personal data must be 'accurate and, where necessary, kept up to date' and that 'every reasonable step must be taken to ensure that personal data that are inaccurate […] are erased or rectified without

[18] See also the A29WP Guidelines on Data Protection Officers published on 13 December 2016, as last revised and adopted on 5 April 2017.
[19] See the A29WP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of the GDPR, published on 4 April 2017.

delay'. Moreover, the GDPR gives consumers the right to dispute the accuracy of personal data held about them and to have errors corrected.

41. This risk is also further mitigated, to some extent, by the requirements under the GDPR to inform consumers where data from external sources are used (see Article 14 of the GDPR) and by the requirements regarding profiling activities, as set out in Article 22 of the GDPR. In particular, the GDPR requires firms using profiling to inform consumers about 'the logic involved' and 'the envisaged consequences of such processing' (Articles 13(2)(f) and 14(2)(g)) and to ensure that consumers are able to 'obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision' (Recital 71 and Article 22(3) of the GDPR).

42. The Recitals to the GDPR further clarify that the principle of fair and transparent processing implies that firms using profiling should implement appropriate mathematical or statistical procedures for the profiling as well as appropriate technical and organisational measures to enable inaccuracies in personal data to be corrected and minimise the risk of errors, and to prevent discriminatory effects based on certain sensitive data, such as health data (Recital 71 of the GDPR).

43. In addition to the requirements under the GDPR, the AMLD requires financial institutions to take know-your-customer measures, including ongoing monitoring of the business relationship with their customers so as to ensure that the transactions performed are consistent with the financial institution's knowledge of the customer, its business and its risk profile and to ensure that customers' data are kept up to date (see Article 13 (1)(d) of the AMLD).

44. Furthermore, the MCD imposes qualitative requirements on banks' credit quality assessments and scoring systems (see, for example, Articles 18 and 20 of the MCD)[20] and requires creditors to inform consumers in advance if they intend to consult a database for the creditworthiness assessment. In the event of rejection of a credit application, the MCD requires creditors to inform consumers whether the rejection is based on automated processing of data or on the consultation of a database and, in the latter case, to further inform the consumer of the result of such consultation and of the particulars of the database consulted (Article 18(5)(c) and (d) of the MCD). Similar disclosure requirements are also included in the Consumer Credit Directive (see Article 9)[21].

45. As regards the risk of lock-in identified in the DP, the new provisions on data portability under the GDPR aim to address this risk and to further strengthen consumers' control over their personal data. In particular, Article 20 of the GDPR allows consumers, where the processing of personal data is carried out by automated means, to receive the personal data that they have provided to a data controller 'in a structured, commonly used and machine-readable format', to store those data for further personal use or to transmit the data to

[20] See also EBA Guidelines on creditworthiness assessment, published on 1 June 2015, in support of Article 18 of the MCD, and applicable from 21 March 2006.
[21] Directive 2008/48/EC on credit agreements for consumers

another provider. Consumers may also request a data controller to transmit those data directly to another provider, where this is technically feasible[22].

46. The Guidelines on the right to data portability issued by the A29WP provide further guidance on the conditions under which this right applies. They clarify, for example, that this right applies only where the processing is based on the data subject's consent or the necessity to perform a contract (as a legal basis for the processing). The Guidelines also state that data considered to have been 'provided' by the data subject include not only data that a person knowingly and actively shared (such as online forms), but also personal data resulting from the observation of that person's behaviour (such as his or her search history, traffic data and location data); in contrast, 'inferred data' and 'derived data', which are obtained from subsequent analysis of a person's behaviour, such as 'the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules)' are not covered by the right to data portability[23].

47. Furthermore, in addition to the GDPR, other sectoral EU regulations, such as the PAD and the PSD2 provisions on access to account data, aim to attenuate the risk of lock-in. In particular, the PAD aims to make it easier for consumers to compare payment account offerings, to facilitate the switching of payment accounts and to ensure that all consumers legally resident in the EU have access to a basic bank account. Building on what has already been achieved through the PAD for payment accounts, the European Commission has indicated in its Action Plan on Retail Financial Services[24] that it will explore further steps to make it easier for consumers to switch to more advantageous retail financial services.

48. Also, the UCPD and the Directive on Unfair Contract Terms [25] prohibit abusive marketing practices seeking to oblige consumers to pay for a service they have not solicited ('inertia selling'), and automatic, tacit renewals of contracts, where the deadline for the consumer to express his or her choice not to extend the contract 'is unreasonably early".

49. As regards the risk of data being used for aggressive commercial practices, the UCPD aims to mitigate such risks, by prohibiting aggressive commercial practices, such as cold calling or unwanted e-mails (see Annex 1 (26)). It also protects consumers against misleading commercial practices, such as the omission of key information (regarding for example the manner in which the price is calculated or the motives behind the commercial practice), that the average consumer needs in order to take an informed transactional decision, and whose omission thereby causes, or is likely to cause, the consumer to take a transactional decision that he or she would not have taken otherwise.

50. For example, a provider's failure to inform a consumer that the data he or she provided in order to access the service will be used for commercial purposes could be considered a misleading omission of material information prohibited by the UCPD. Furthermore, as shown

[22] In this respect, Recital 68 to the GDPR encourages data controllers to develop interoperable formats that enable data portability, but without creating an obligation for controllers to adopt or maintain processing systems that are technically compatible.
[23] See the Guidelines on the right to data portability published by the A29WP on 13 December 2016 and revised on 5 April 2017.
[24] See the Communication from the Commission 'Consumer Financial Services Action Plan: Better Products, More Choice', published on 23 March 2017.
[25] Council Directive 93/13/EEC on unfair terms in consumer contracts

in the European Commission's Staff Working Document from 2016 providing guidance on the application of the UCPD, the provisions of the UCPD may become applicable to practices such as dynamic pricing (where the price of a product is changed in a highly flexible and quick manner in response to market demands), price discrimination (where different groups of consumers are charged a different price for the same products or services) or personalised pricing (where the pricing is based on the tracking and profiling of the consumer's behaviour)[26].

51. In addition, the E-Privacy Directive[27] and the Distance Marketing of Financial Services Directive[28] contain provisions that aim to counter aggressive practices such as sending unsolicited communications for direct marketing purposes. In particular, the E-Privacy Directive requires providers to obtain consumers' prior consent, for direct marketing communications by means of automated calling, e-mails or SMS messages ('opt-in'). An exception (known as 'soft opt-in') applies to marketing communications sent via e-mail, within the context of an existing customer relationship, for similar products and services, provided certain conditions are met, as set out in Article 13(2) of the E-Privacy Directive. The pending revision of the E-Privacy Directive is also expected to result in greater alignment with the GDPR, including in relation to provisions on the use of cookies and other hidden identifiers/profiling[29].

52. Furthermore, in the financial services sector, there are specific rules that aim to mitigate the risk of consumers being targeted for products that are not in their best interest, such as the provisions under the MCD requiring creditors and credit intermediaries under the MCD, to 'act honestly, fairly, transparently and professionally, taking account of the rights and interests of the consumers' (see Article 7 of the MCD). The MCD also sets high standards for advisory services, or personal recommendations made to a consumer as regards credit agreements that fall under the scope of the MCD, by requiring the entities allowed to perform such services to act in the consumer's best interest and to recommend credit agreements suitable to his or her needs, financial situation and personal circumstances.

53. In addition to the MCD, the EBA has adopted own-initiative Guidelines on product oversight and governance (POG) arrangements applicable to manufacturers and distributors of retail banking products that fall within the EBA's regulatory remit (i.e., mortgages, personal loans, deposits, payment accounts, electronic money and payment services)[30] and Guidelines on remuneration policies and practices related to the sale and provision of retail banking

[26] See the Commission Staff Working Document 'Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices' published on 25 May 2016. The distinction between the three types of pricing practices mentioned is based on the Commission Staff Working Document.
[27] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ('E-Privacy Directive') – currently under review by the European Commission.
[28] Directive 2002/65/EC concerning the distance marketing of consumer financial services
[29] See the European Commission's proposal for a Regulation on Privacy and Electronic Communications published on 10 January 2017.
[30] See the EBA Guidelines on product oversight and governance arrangements for retail banking products, published on 15 July 2015 and applicable to retail banking products brought to the market after 3 January 2017 and to existing products that are significantly changed after this date.

products and services[31], which aim to mitigate the risk of consumers being targeted for unsuitable products that are not in their best interest.

54. In relation to the security risks identified in the DP, several pieces of legislation aim to mitigate such risks. For example, the GDPR requires that data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage' (Article 5(1)(f)) and introduces strict requirements regarding notification of data breaches to the DPA and, in certain cases, to the individuals concerned (Articles 33 and 34 of the GDPR).

55. Furthermore, several sectoral legislative measures adopted in recent years aim to mitigate security risks. These include the NIS Directive, adopted on 6 July 2016, which introduced new cybersecurity requirements for businesses in certain sectors (including the banking sector) that are identified by Member States as 'operators of essential services' and requires key digital service providers (search engines, cloud computing services and online marketplaces) to comply with the security and incident notification requirements under the NIS Directive.

56. Also, further initiatives at EU level have been taken in recent years in order to increase security in the financial services sector, such as the EBA own-initiative Guidelines on the security of internet payments under the PSD1[32] and the security requirements under the PSD2, which will apply to all PSPs, including banks, payment institutions and e-money institutions. These requirements will be further developed in the technical standards and guidelines that the EBA has been mandated to issue in the implementation of the PSD2 and include:

    - the implementation of strong customer authentication for electronic payments across all EU Member States and of common and secure communication standards, through which the new TPPs will interact with, and securely access the customer payment accounts held with, banks, as well as the requirement for all PSPs to have in place risk and fraud monitoring (e.g. transaction risk analysis) capable to identify any unusual payment patterns, as required by PSD2 and the draft Regulatory Technical Standards (RTS) under Article 98 of the PSD2[33];
    - the new requirements regarding the management of operational and security risks under Article 95 of the PSD2 and the EBA guidelines on security measures to address operational and security risks under the PSD2[34]; and
    - the new requirement to report major security and operational incidents under Article 96 of the PSD and the EBA Guidelines on major incident reporting under the PSD2[35].

[31] See the EBA Guidelines on remuneration policies and practices related to the sale and provision of retail banking products and services, published on 28 September 2016 and applicable from 13 January 2018.
[32] See EBA Guidelines on internet payments security published on 19 December 2014 and applicable from 1 December 2015.
[33] See the final draft of the EBA RTS on strong customer authentication and common and secure communication under Article 98 of PSD2, submitted on 23 February 2017 to the European Commission, and the Commission's announced intention to amend the draft RTS.
[34] See the draft EBA Guidelines on security measures for operational and security risks under PSD2, published for consultation on 5 May 2017.
[35] See the draft EBA Guidelines on major incidents reporting under PSD2, published for consultation on 7 December 2016.

57. In addition to the above, in the banking sector, the EBA has issued own-initiative Guidelines to competent authorities on the assessment of information and communication technology (ICT) risk of credit institutions and investment firms, as part of the Supervisory Review and Evaluation Process (SREP)[36] as well as draft Recommendations on outsourcing to cloud service providers[37]. The Recommendations on outsourcing to cloud service providers are addressed to national competent authorities, credit institutions and investment firms and complement the Guidelines on outsourcing developed by the Committee of European Banking Supervisors[38]. They cover five key areas: the security of data and systems; the location of data and data processing; access and audit rights; chain outsourcing; and contingency plans and exit strategies.

58. As regards the concerns expressed by some respondents regarding the potential lack of a level playing field, the EBA notes that several existing pieces of legislation aim to alleviate, to some extent, this risk. In particular, the GDPR, together with the E-Privacy Directive, will provide a comprehensive legal framework on the processing of personal data that will apply to both financial and non-financial service providers and will also require companies based outside the EU, including social media providers, internet marketplaces and similar internet based platforms, to apply the same data protection rules as European companies if they are processing personal data about individuals in the EU in connection with the offering of goods and services, or monitoring individuals' behaviour.

59. In addition, the new security requirements under the PSD2 may further attenuate some of the concerns expressed by respondents by requiring that the same security requirements should be implemented by all PSPs, subject to the proportionality principle, whether these are banks or the new TPPs providing AIS or PIS services.

60. Finally, the EBA notes that these concerns are also part of the ongoing policy discussions on the broader topic of FinTech that are taking place at EU level, for example, by the European Commission[39] and the European Parliament[40], and will continue to follow closely the developments on this topic following the Commission's recent Consultation Paper on FinTech[41].

[36] See the EBA Guidelines on the ICT risk assessment under the Supervisory Review and Evaluation process (SREP), published on 11 May 2017. The Guidelines will complement, from 1 January 2018, the EBA SREP Guidelines, published on 19 December 2014 and applicable from 1 January 2016.
[37] See the draft EBA draft Recommenadationson outsourcing to cloud service providers, published on 18 May 2017.
[38] See the Guidelines on Outsourcing, published on 14 December 2006.
[39] See for example the Communication from the Commission on 'Building a European Data Economy' and the Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, both published on 10 January2017, as well as the Communication from the Commission on 'Consumer Financial Services Action Plan: Better Products, More Choice' and the Consultation Paper 'FinTech: a more competitive and innovative European financial sector', both published by the Commission on 23 March 2017.
[40] See for example the Report on 'FinTech: the influence of technology on the future of the financial sector', adopted by the European Parliament on 28 April 2017.
[41] See the Commission Consultation Paper 'FinTech: a more competitive and innovative European financial sector', published on 23 March 2017.

E. The risks arising specifically from Big Data analytics are cross-sectoral and will therefore be assessed in forthcoming joint work with ESMA and EIOPA

61. Some respondents, and in particular consumer associations, were concerned by the risk that consumers may experience discrimination or be excluded from accessing certain financial services, especially in the context of an increased use of Big Data analytics. Consumer associations fear that algorithms may discriminate against those who are less willing to share their data online. They also expressed concerns that customers with limited credit history may face exclusion from access to financial services if the algorithm used to assess creditworthiness draws heavily on data of successful repayment of previous loans, as opposed to an analysis of spending patterns and ability to save.

62. Consumer associations were also of the opinion that, although, in their opinion, the US data protection regulation is weaker than that of the EU, similar risks that have materialised in the USA may be worth being analysed in Europe as well. They made references, for example, to the study carried out in 2014 in the USA by the National Law Consumer Center (NCLC), which concluded that 'the use of big data in the lending area does not appear to result in more affordable products for low-income consumers'[42]. Industry stakeholders, on the other hand, argued that such risks have not materialised in the EU and that it would not be in the interest of financial institutions to exclude certain customer segments from the provision of financial services.

63. Consumer associations also see a risk that if Big Data will become commonly used in risk assessments, consumers may seek to artificially improve their 'scores' by tampering with their online data, and that the high volume of data used in Big Data analytics increases the probability of inaccuracies.

64. Some respondents also expressed concerns that, by using predictive analytics, financial institutions may rely on decisions where they may not be able to prove causality between input data and decision, making the credit scoring and decision-making process non-transparent[43]. Consumer associations also expressed concerns regarding risks of price discrimination and that firms may use Big Data to 'optimise' the price of their products, by estimating more accurately the price increase a consumer would accept before they switch to a different provider.

65. The EBA acknowledges these concerns. Given that similar concerns have been raised in respect of Big Data analytics in the insurance and investment sectors, the EBA will further consider them as part of the related work on Big Data carried out jointly with the other two ESAs (ESMA and EIOPA)[44].

[42] 'Big data: a big disappointment for scoring consumer credit risk', US National Consumer Law Center, March 2014, p. 33.
[43] One respondent gave the example of an online lender provider that is reported to use around 20 000 data points in its credit scoring algorithm, which may make it more difficult to give consumers an indication of the reason why they are declined for credit.
[44] See the Discussion Paper on the use of Big Data by financial institutions, published by the JC on 19 December 2016.

F. Given the application of EU law currently in force, the EBA finds no sufficient grounds for further industry-specific legislative interventions on this matter at this point in time, but will continue to monitor closely the evolution of this innovation

66. Taking into account the application of existing EU law and considering that most of the risks identified in the DP seem to be sufficiently mitigated by several legal provisions currently in force and generally applicable to the management and utilisation of consumer data by financial institutions, some of which, such as the GDPR and the PSD2 have not yet been fully applied across the EU, the EBA finds no sufficient reasons at this stage for additional industry-specific legislative interventions within the financial sector.

67. However, given that the market is rapidly evolving and innovative uses of customer data are expanding, the EBA will continue to monitor this innovation and engage in further cooperation with the other ESAs, the European Commission and EU data protection supervisors. As part of its ongoing monitoring work, the EBA will look at concrete case studies, including the use of social network data and other external data for credit scoring analytics, and will continue the work on Big Data together with the other two ESAs[45].

68. The EBA will also further look into potential regulatory barriers to the development of innovative uses of data that may fall within the EBA's regulatory remit and, in particular, to the concerns raised by respondents regarding legal uncertainty.

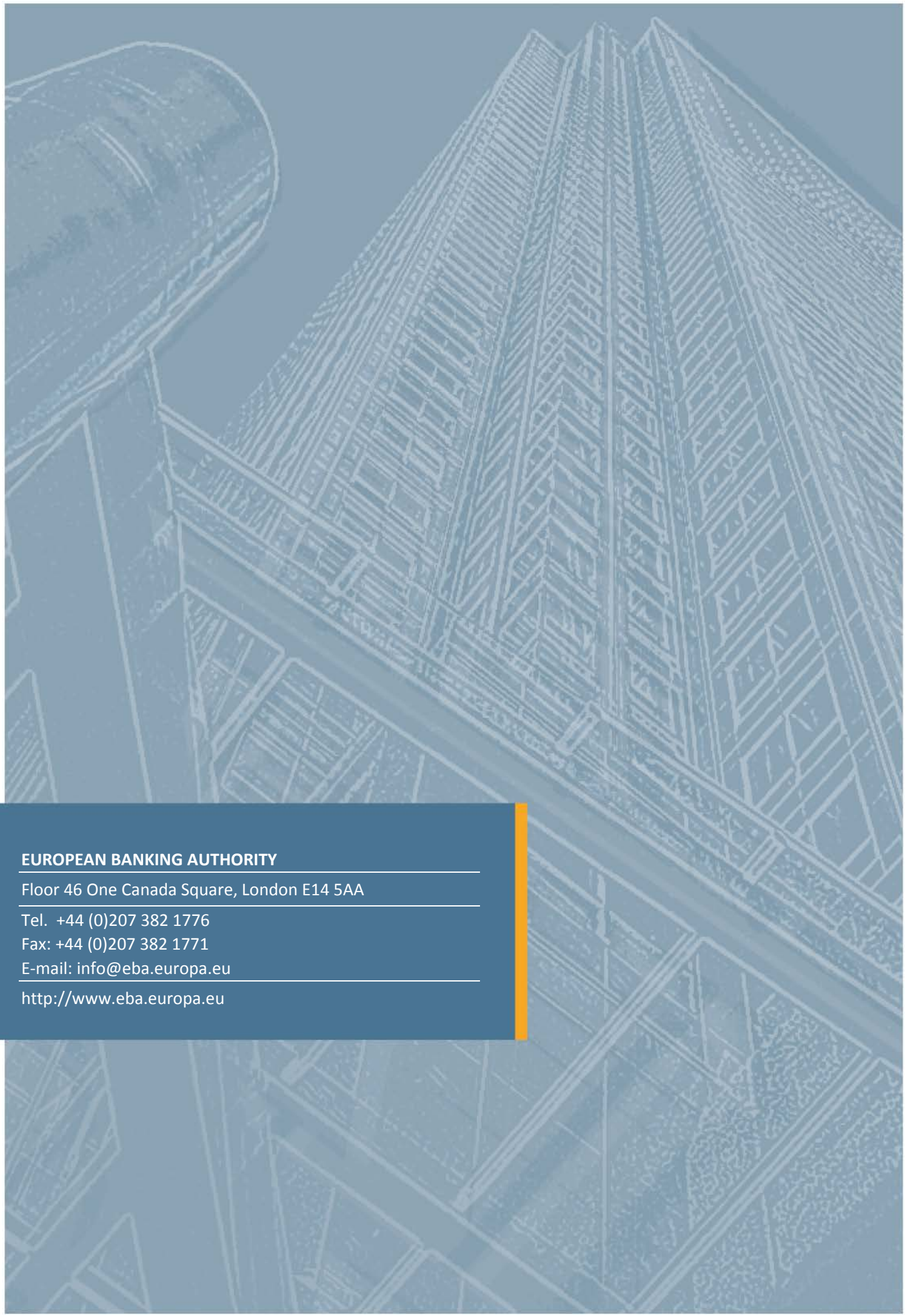
69. Given the EBA's objective of regulatory convergence across the EU, prevention of regulatory arbitrage and promotion of consumer protection, the EBA has an interest in seeing the GDPR applied consistently across the financial services markets within the 28 Member States. To that end, the EBA stands ready to support any data protection initiatives by the A29WP and the EDPS that would provide more clarity on the application of the GDPR in the financial services sector.

70. The EBA also strongly encourages cooperation between supervisors across all relevant policy areas in order to provide more legal certainty to market participants and ensure a consistent supervisory approach. Cooperation between supervisory authorities at international level may also be beneficial in order to harness the full potential of innovative uses of data and help anticipate or mitigate certain risks.

71. In addition to the regulatory framework, financial literacy and education initiatives also have an important role to play in mitigating the risks identified, by increasing consumers' knowledge about the innovative products and services, how their data are being used to build such services and their legal rights. The EBA encourages such initiatives and considers that they should raise consumer awareness as regards both the opportunities and the risks related to innovative uses of consumer data (such as the risk of hyper-consumerism or misselling practices).

[45] Ibid.

72. The EBA will also be carrying out additional work in 2017 to look at the prudential and consumer impact, as well as any authorisation perimeter issues arising from new FinTech innovations, and will update its conclusions as and when necessary.



EUROPEAN BANKING AUTHORITY

Floor 46 One Canada Square, London E14 5AA

Tel. +44 (0)207 382 1776
Fax: +44 (0)207 382 1771
E-mail: info@eba.europa.eu

http://www.eba.europa.eu