JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC/2018/04

15 March 2018

Joint Committee Final Report on Big Data

Contents

Acronyms and definitions

AIFMD	Alternative Investment Fund Manager Directive (2011/61/EC)
AMLD	Anti-Money Laundering Directive (2015/849)
CRD IV	Capital Requierements Directive (2013/36/EU)
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
EMD	E-Money Directive (2009/110/EC)
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
GDPR	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (679/2016/EU)
IDD	Insurance Distribution Directive (2016/97/EC)
MCD	Mortgage Credit Directive (2014/17/EU)
MiFID II	Markets in Financial Instruments Directive (2014/65/EC)
NIS	Directive concerning measures for a high common level of security of network and information systems across the Union (2016/1148/EU)
PSD	Payment Services Directive (2007/63/EC)
PSD2	Revised Payment Services Directive II (2015/2366)
PSPs	Payment service providers
UCPD	Directive concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) (2005/29/EC)

1. Overview

1. One of the tasks of the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), collectively referred to as the European Supervisory Authorities (ESAs), is to monitor any emerging risks for consumers and financial institutions as well as new and existing financial activities and to adopt measures, where needed, with a view to promoting consumer protection and the safety and soundness of markets and convergence in regulatory practices. The coordination of the ESAs' actions in these areas takes place within the Joint Committee.

2. In monitoring consumer protection developments and financial innovations, the ESAs have noted the continued increase in the use of Big Data, albeit to varying extents, across the banking, insurance and securities sectors and across different EU Member States.

3. As a consequence, the 2016 Work Programme of Joint Committee of the European Supervisory Authorities[1] mandated its Sub-Committee on Consumer Protection and Financial Innovation to work on the opportunities and challenges of the use of Big Data by financial institutions.

4. On 19 December 2016, the Joint Committee issued a Discussion Paper on the use of Big Data by financial institutions[2].

5. Stakeholders were asked to respond to the questions raised in the Discussion Paper by 17 March 2017.

6. A total of 68 responses were received. Public responses are published on the ESMA's website.[3]

2. Contents

7. Section 3 of this Final Report contains an executive summary summarising the key aspects of the various sections of the Final Report.

8. Section 4 contains a detailed feedback statement which summarises, through the angle of 12 key topics, the feedback received from stakeholders and the ESAs' reaction in response to some of the issues raised by respondents.

9. Most of the comments made by the ESAs in Section 4 (ESAs' reaction) are further developed in Section 5 which sets out the ESAs conclusions including a reference to some existing requirements deriving from European financial

1 2016 Work Programme of Joint Committee of the European Supervisory Authorities - Available here.
2 Joint Committee Discussion Paper on the use of Big Data for Financial Institutions – Available here.
3 Available here.

and non-financial legislation which are relevant to the use of Big Data techniques by financial institutions as well as a list of items that could be used by financial institutions to develop good practices in relation to the use of Big Data.

3. Executive summary

10. The responses received from stakeholders generally coincided with the content of the Discussion Paper, particularly with regards to the challenges and opportunities identified. Yet, the feedback received enabled to nuance some of the statements contained in the Discussion Paper and to better inform the ESAs assessment of the use of Big Data across the three sectors and its impact on the financial sector as a whole.

11. The respondents generally agreed with the tentative definition and description of the Big Data phenomenon provided in the Discussion Paper, while highlighting that any definition of a fast evolving phenomenon such as Big Data should remain flexible to accommodate inevitable adjustments.

12. The respondents noted that the accuracy of the data used in Big Data analyses is of utmost importance and expressed concerns regarding practices that do not guarantee the accuracy of the data collected (such as the gathering of data from social media), which could lead to erroneous decisions based on this inaccurate data or on spurious correlations arising from it. There was however a quite wide agreement on the fact that the entry into application of new legislation including the GDPR[4] (General Data Protection Regulation) will help mitigate risks in this field.

13. Many respondents raised concerns regarding the potential consequences of the increasing level of segmentation of customers enabled by Big Data on the comparability availability, affordability and pricing practices of products and services, although to date there is limited evidence of such risks materialising. Some respondents pointed out the overarching obligation of financial institutions to treat customers fairly and the need to ensure that sensitive data are only used based on the consumers' informed consent and only for limited purposes. Some stakeholders also warned that consumers may not be fully aware of Big Data tools being used and stressed the need to increase transparency for consumers to enable them to better understand and control the use of their data.

14. A number of respondents also highlighted that the growing use of Big Data could increase the breadth of the consequences of cyber risks attacks. On this issue, the ESAs clarify that a number of requirements have been enacted in recent years at the European level aiming at the prevention of cyber risks. This Final Report also highlights the existence of European Union legislation specifically aiming at tackling information and systems risks.

15. Respondents also highlighted the numerous benefits arising from Big Data. A large number of respondents (across the three sectors) agreed that the

4 The GDPR will enter into application from 25 May 2018.

use of Big Data techniques could help financial institutions to develop products better tailored to the needs of their target market and support the implementation of product governance and foster the development, distribution and monitoring of products, as well as the broader supervision of product governance requirements. Other benefits arising from Big Data highlighted by respondents included enhancing the efficiency of the internal procedures inside the organisations, improving the fight against fraud, or enabling better customer-client interactions.

16. The feedback received from respondents confirms and reinforces the need for regulators and supervisors to continue monitoring closely the development of Big Data techniques and their use by financial institutions. This monitoring should focus on the aspects that have been identified as bearing the strongest risks.

17. In this Final Report, the ESAs highlight the relevance of a number of existing requirements in the sectorial financial legislation as well as in other relevant areas (such as data protection, cyber security and consumer protection). The ESAs believe that the legislative requirements existing in these areas constitute an already quite solid framework to mitigate the risks identified in the context of this work. The ESAs also note that this framework will be further strengthened with the entry into application of several key pieces of legislation in the financial sector (e.g. IDD, MIFID II, PSD2) as well as in the data protection sector (notably, GDPR). The ESAs will monitor how and to which extent these additional requirements will contribute to mitigate further the risks identified in the context of this work.

18. The ESAs consequently consider that a legislative intervention at this point would be premature, given that some key pieces of legislation are yet to be implemented or have just entered into application. However, the ESAs believe that it is very important for supervisors across various policy areas to coordinate better to ensure that these requirements are effectively complied with.

19. The ESAs also invite financial institutions to develop and implement good practices on the use of Big Data in order to promote a fair, transparent and non-discriminatory treatment of consumers and to ensure that Big Data strategies are designed in a responsible way and are fully aligned with the interests of consumers. To this end, the ESAs suggest an indicative a list of arrangements and behaviours that could be followed by financial institutions to develop good practices on the use of Big Data. The ESAs propose items in three keys area, namely (i) “Robust Big Data processes and algorithm”, (ii) “Consumer Protection” and (iii) “Disclosure on the use of Big Data”.

4. Feedback statement

A. Description of the Big Data phenomenon

i. Description of the phenomenon and state of implementation across financial institutions

20. Most respondents (across sectors) agreed with the description of Big Data suggested in the Discussion Paper,[5] which notably referred to the 3 "Vs", standing for "Volume", "Variety" and "Velocity"[6]. Some stakeholders however also suggested a definition following a 4 or 5 V approach (for "Veracity" and/or "Value"). It was also pointed out that Big Data refers to processing of data sets so large and complex that they cannot be handled by traditional data processing software. Several respondents also commented that any definition of a fast evolving phenomenon such as Big Data should remain flexible to accommodate the inevitable need for future adjustments.

21. For some stakeholders, the Big Data phenomenon is not new and Big Data tools have already been used for several years. For others, it is a new phenomenon with applications in the financial sector still at an early stage.

22. Most respondents across the three sectors agree that Big Data may have an impact on almost all financial institutions and on their products and services. Certain respondents stated that the impact of Big Data would be specifically strong for Fintechs or financial institutions that can afford the initial costs as well as big consulting/technology companies that can offer analytical services. From a broader perspective, respondents generally agreed that Big Data may be an important factor of economic competitiveness.

23. For certain respondents the main areas of application of Big Data observed so far concern the improvement of the understanding of consumers' preferences. Based on improved information (for instance from personal devices/online data, etc.) product/service providers strengthen the feedback loop between them and consumers. This may lead to increased personalisation of products and services as well as more accurate consumer profile/risk assessments. Several respondents mentioned further examples of the use of Big Data: increasing sales of pay as you drive or pay as you live insurance (also known as "usage-based insurance"); increased personalisation of risk assessment; credit scoring using broad ranges of data; fraud management; increased use of robo-advice. Certain respondents also

5 Joint Committee Discussion Paper on the use of Big Data by Financial Institutions (Page 7) – Available here.
6 The first "V", "Volume", refers a large volume of data. The second "V" stands for "Variety" refers to the variety of data as the result of the combination of different datasets and sources. The third "V" "Velocity" refers notably to the speed of data processing.

saw potential in the areas of claims handling, fraud detection, pricing, risk selection and underwriting.

ii. Type and sources of data and IT tools

24. A few banking and insurance respondents mentioned that most data stems from internal sources and, in comparison, data from external sources would play a minor role. Some insurance respondents noted that by nature the industry requires the processing of large amounts of data; a few also noted the recent increase of the use of external data sources or of climate data. Other stakeholders provided examples of different types of data they use: credit history, behavioural data, consumer habit data, statistical data and data found in broader networks, individual data as well as aggregated data. However, the collection of data, such as on online behaviour and geolocation, going beyond the range of data required to provide usual financial services was also pointed out.

25. Respondents across sectors stated that they use Big Data applications developed both internally and externally. Several securities markets stakeholders stated that they get external software support, but already have or are going to develop their algorithms and analytics internally.

B. Level playing field and fair competition

26. For some respondents, the use of Big Data could contribute to ensuring a level playing field (e.g. by allowing smaller companies to compete with larger financial players or to exploit their data resources currently unused) or could lead to interesting cooperation arrangements (e.g. between financial institutions and Fintech companies).

27. On the contrary, a number of respondents, particularly from the banking sector, were critical with respect to what they perceived as possible regulatory arbitrage or an unlevel playing field between regulated financial institutions and Fintech start-ups and other technology firms. For instance, some of these respondents pointed out that some Fintech start-ups and other large technology firms fall outside the remit of financial legislation rules and therefore do not need to comply for example with restrictions concerning the use of cloud solutions, prudential requirements or remuneration rules.

28. A number of respondents consequently noted that in order to maintain a fair competition among various players, it is important to ensure that the principle of "same business, same rules" is respected, and that any potential regulatory or supervisory measures should remain technology neutral in order to foster innovation and level playing field. Some were also critical towards regulatory sandboxes developed by certain NCAs, for similar reasons.

29. From a different perspective, other stakeholders mentioned the existence of obstacles to fair competition between market players resulting from the creation of data oligopolies by some categories of stakeholders and the difficulties to access data by others. These stakeholders expressed the view that data is becoming a key competitive factor that could undermine competition in the markets if not all actors have the same opportunities to access certain types of data. They illustrated their point referring to information on driving behaviours, vehicle condition or geolocation collected by car manufactures through the increasing penetration of connected vehicles and telematics and potentially not accessible to insurance companies and other interested stakeholders.

30. Some respondents noted that beyond the regulatory arbitrage issues mentioned above, some other non-regulatory factors (e.g. distortions by important data providers through unfair pricing, availability of qualified staff, tackling legacy issues, technological and reputational risks) could also interfere with the fair competition among market participants using Big Data technologies. Some respondents accordingly suggested to include references to competition rules in the section on the relevant regulatory framework.

ESAs' reactions

31. The ESAs acknowledge the concerns expressed by respondents and intend to continue monitoring the development of the market, notably with a view to encouraging and, when within their remit, ensuring a level playing field among players in the market.

32. However, the ESAs would like to highlight that several existing pieces of legislation address, to some extent, the concerns raised by respondents regarding the lack of a level playing field. The GDPR, which among other provisions includes the principle of data portability, notably will apply to all service providers processing personal data of European Union individuals, irrespective of whether they are financial institutions or non-regulated entities. The GDPR also recognises the principle of data portability which should help mitigate 'lock-in' effects for consumers. Also, the PSD 2 will bring into its scope new providers that were previously unregulated by European financial legislation, such as account information service providers. Such providers will be subject to new and harmonised rules at EU level, which should mitigate some of the concerns on consumer protection, security and competition that respondents mentioned.

33. On these issues, the ESAs will continue engaging with the other regulators and supervisors, both at European and national levels.

C. Impact of Big Data on financial inclusion, comparability and pricing practices

34. Respondents across sectors provided examples of products and services that would be impacted by Big Data. These examples confirmed that the granular segmentations of consumers enabled by Big Data have a number of impacts on aspects such as marketing campaigns, pricing practices, contextual offers (e.g. cross-selling), individualised products and services, credit and risk scoring / segmentation, fraud prevention, etc.

i. Impact on financial inclusion

35. An important number of respondents agreed that Big Data is likely to have positive implications on the availability and affordability of financial products and services for some consumers. For example, some stakeholders pointed out that Big Data may enhance access to financial services for clients with limited financial/ credit history. Respondents mentioned the example of the use of wearable telematics devices to improve how chronic conditions, such as diabetes, are managed and used to reduce the risk of disability, thus improving the access to insurance for such consumers. Also, a majority of respondents agreed that Big Data techniques allowed a better understanding of customer behaviour, which could help firms to better adapt to needs of specific clients groups, such as millennials.

36. On the other hand, some respondents (representing consumer organisations but also professional associations) considered that, in competitive markets, Big Data could have significant negative effects on the availability and affordability of financial products and services for some consumers with higher risk profiles or about whom only little data is available due to their limited digital/online activities. Furthermore, a marketing segmentation that is too granular may limit the choice of products and services offered to some consumers. Consumers mentioned that assessing risks more granularly could result in changes to terms and conditions offered to consumers, especially when risks cannot be easily avoided. These stakeholders gave the example of owners or tenants located in geographical areas exposed to a high risk of flooding that may face difficulties to obtain a house insurance coverage.

37. For some stakeholders, certain conditions have to be fulfilled to achieve progress on affordability and availability of financial services using Big Data. These conditions include potential supervisory and regulatory actions, such as monitoring of algorithms and improving the standardisation of data to facilitate its use for online (e.g. aggregators/comparative) tools. A few respondents also highlighted that personal advice by intermediaries would be necessary to make the benefits materialise.

ii. Impact on the capacity to compare financial services and products

38. A significant number of industry stakeholders were of the view that Big Data could allow consumers to benefit from effective comparison websites or robo-advice that would help them understand/select across various products/services. Moreover, legislation such as MiFID, IDD, PRIIPs, MCD and PAD will contribute to facilitating comparison/ switching of products and services for consumers.

39. Some other respondents (including consumer representatives) expressed the view that the increasing individualisation of products and services would reduce the capacity to compare between products/services. These respondents also considered that risks will be heightened with the further development of AI/machine learning and the opacity of algorithms (making it more and more difficult for firms to explain the logic of decisions/services or products offered to clients). The capacity to compare products/services could be further diminished also in cases of firms applying different Big Data tools to similar offers, thereby increasing information asymmetry to the detriment of consumers.

40. Some respondents consider that it is the task of the market to solve potential issues of incomparability, as more experience with the use of Big Data is gathered, but that in case the market will not be able to solve these comparability issues, guidelines or standardisation mechanisms for data/comparison tools may become necessary to mitigate these issues.

41. A consumer organisation noted that from a broader perspective, an European-wide framework for simple, transparent and cost effective financial products could limit the potential negative impact of Big Data through enhancing transparency and competition.

iii. The impact on pricing practices

42. Some respondents consider that Big Data may support more adequate risk pricing or cheaper premium for car insurance for certain drivers, which could benefit consumers. By contrast, other respondents consider that Big Data increases the risk of treating consumers unfairly, for example, by offering the same service with different prices depending on clients' behaviours ("price optimisation"). This may be detrimental for consumers, especially if behavioural biases (such as limited time, resources or financial capabilities of consumers) are exploited.

43. Some respondents also highlighted the emergence of new moral hazard risks related to the use of Big Data. In particular, they saw a risk, against the backdrop of increased segmentation and price optimisation that some

consumers may potentially seek to artificially improve their ratings either by paying online reputation management companies or by tampering with data generated about them, and tailor their profiles with data that is "helpful" to them.

44. In the view of some respondents, the development of aggregators and comparators could mitigate these risks by empowering investors to compare prices. Some stakeholders believed that existing rules are sufficient to address these concerns. In comparison, others considered that competition and innovation would bring solutions, notably by developing services to help clients feel more empowered or compare products and prices applied. Conversely, consumer representatives (but also some industry associations) had more reserved views and considered that there may be a need to further monitor developments on this point.

45. In this context, some respondents see a need for regulation which tackles especially discrimination and inappropriate price optimisation, and believe that the use of Big Data techniques to adjust marketing and pricing for similar clients should be monitored.

46. Also, several respondents suggested that supervisory authorities should make use of Big Data tools to their advantage (to monitor behaviours in the market and risks).

ESAs' reactions

47. In light of the above feedback, as well as gathered evidence, the ESAs will further assess, in each of their respective sectors, whether there is a need to further monitor the impact of highly granular segmentations on access and availability of certain financial services and products, as well as whether there is merit in monitoring the development of tools able to mitigate potential negative effects.

48. The ESAs will also assess, where relevant, in each of their respective sectors, whether there is merit in further monitoring how firms' pricing practices and rating factors are designed and operate in practice, as well as the drivers, types of systems and data that firms use to set the final price to consumers.

49. In addition to compliance with applicable legal requirements (in particular the requirement to treat customers fairly), the recommendations set out in Section 5 below aim to incentivise financial institutions to take into account the interests of consumers when developing products based on Big Data and tackle, or at least mitigate, the potential negative impacts of a highly granular segmentation of customers enabled by the use of Big Data techniques.

D. Potential shortcomings in the transparency of Big Data tools

50. A few respondents were of the view that the Discussion Paper failed to acknowledge that predictions based on Big Data can be flawed. It was also noted that machine learning and the development of artificial intelligence could render the decision-making process less transparent and, in general, the intensity of the risks listed in the Discussion Paper could increase as a direct consequence of such new tools.

ESAs' reactions

51. The ESAs acknowledge that these issues deserve closer monitoring going forward, and that it is important for both ESAs/NCAs and financial institutions to develop capacities to be able to test methodologies of Big Data processes in order to prevent biases and flaws.

E. Accuracy of data - Fair and transparent use of data collected

52. Beyond issues linked to Big Data algorithms as such, a significant number of stakeholders highlighted that the performance of Big Data tools depends heavily on the reliability of the data used. These respondents cautioned that errors or biases in algorithms remain possible and can impact customers. For example, large amounts of data may lead to new correlations between different things, but correlation does not mean causation and may lead to incorrect decisions based on them.

53. In addition, some stakeholders pointed out the need to ensure that sensitive data are used only based on the consumers' informed consent, and only for limited purposes. Some stakeholders also warned that consumers may not be fully aware of Big Data tools being used (e.g. in case of use of box ticking agreements) and stressed the need to increase transparency for consumers to enable them to better understand and control the use of their data.

54. Some respondents also suggested that a broader discussion should take place in order to determine which types of data should be allowed to be used from an ethical point of view and on whether there may be types of data that are allowed by existing regulation but are against the consumers' interest or need clearer approval from the consumer.

55. On the other hand, several respondents were of the view that data protection requirements (especially GDPR) will provide a sufficient framework for Big Data, because these requirements are sector neutral and address most of the risks identified. While stakeholders acknowledged that data protection is

not within the remit of the ESAs, some respondents believed that further guidance on the implementation of the GDPR is needed to take into account the needs of the financial industry and consumers, enhance legal certainty and foster security and trust of market participants in Big Data based products and services. Also, some respondents expressed the view that cooperation on the use of data in financial services between banking supervisors, data protection authorities and financial intelligence units should be improved.

ESAs' reactions

56. The ESAs note that the GDPR sets sector neutral requirements which apply to any person processing personal data of individuals in the European Union[7]. In addition, as pointed out by a number of respondents, the GDPR does not fall in the remit of the ESAs. This means that the ESAs are not positioned to issue opinion on the way the GDPR should be interpreted, applied or enforced. Nevertheless, the ESAs acknowledge the need to further engage with data protection supervisors to explore ways to provide further guidance to both consumers and financial institutions.

57. The ESAs note that the entry into application of the GDPR, as of May 2018, will increase the requirements currently applicable in relation to data accuracy[8] and enhance data protection and that this may potentially mitigate the risks identified in relation to data protection including data accuracy.

F. Cyber risks

58. A large number of respondents agreed that cyber risks in general should be regarded as a primary source of concern for consumers and market players, since the processed data can be highly sensitive and the impact of cybersecurity breaches can have major consequences. An important number of respondents were of the view that Big Data increases exposure to cyber risks, with detrimental consequences for both consumers and financial institutions. Some respondents noted that this was due to the reception of data from different sources, the use of IT arrangements (including storage and outsourcing in the cloud).

59. Respondents agreed with this view and considered that cyber risks are the same regardless of whether a regular database or a Big Data base is being used, although a few respondents stressed that Big Data could increase the impact of cyber risk related events (and not only the exposure to such cyber risks).

7 GDPR, Article 2.
8 GDPR, Article 5(1)(c).

60. Some respondents mentioned that many institutions were already active in mitigating these risks by developing comprehensive cyber insurance strategies and regularly investing in IT systems aiming at the highest possible security levels and have put in place robust data governance processes.

61. Several respondents across all three sectors stated that cross-sectoral guidance/best practices would be helpful to facilitate the implementation of recently adopted regulations as well as information sharing and other cyber security measures. Respondents also stressed the need to foster collaboration and convergence on data standards, frameworks and methodologies within Europe and at the international level, considering that cyber risks are in essence cross border. Some respondents also highlighted that existing legislation (such as the NIS and GDPR) already addresses cyber risk management.

ESAs' reactions

62. The ESAs stress that financial institutions, to the extent that they are subject to sectorial legislation, are required to have in place measures to ensure continuity and regularity of their services and activities.[9] Therefore, financial institutions are expected to consider cyber risks, including cyber risks associated with the use of Big Data, when setting-up and up-dating their internal policies.

63. The ESAs acknowledge that cybersecurity risks is an important area of growing concern, notably in the financial sector. The ESAs also note that several initiatives, both at European and national levels, have been taken in recent years to tackle this issue. In particular, within the framework of the EU Cybersecurity Strategy, the adoption of the NIS Directive[10] establishes that operators of essential services (including credit institutions and financial market infrastructures) should be required to (i) take appropriate security measures to manage the risks posed to the security of network and information systems that they use in their operations and (ii) notify serious incidents to the relevant national authority[11]. The provisions of the NIS Directive also extend to key digital service providers outside the financial sector, such as search engines, cloud computing services and online marketplaces, which will be required to comply with the security and incident notification requirements under the NIS Directive.

9 Article 16(4) of MiFID II, Article 5(1) of PSD 2, Article 41 of Solvency II.
10 The NIS Directive will enter into force as from 10 May 2018 (Article 25(1) of the NIS Directive).
11 See also EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP): Available here.

64. In addition to the NIS Directive, cyber security and security risks are also addressed under the sectorial legislation as well as GDPR, as further detailed in Section 5 below.

G. Potential systemic risks

65. Some stakeholders expressed concerns in relation to potential systemic risks, notably due to asset price volatility spirals generated by the use of Big Data techniques.

66. More generally, a number of respondents noted the significant reputational risks associated with the application of Big Data tools (especially in case of misuse of consumers personal data, in case of security leaks, erosion of consumers' trust in financial services providers, etc…).

ESAs' reactions

67. The ESAs will further assess, in each of their respective sectors, whether there is a need to consider the possible role of Big Data in the emergence of systemic risks as well as the way Big Data could be used to monitor systemic risks.

68. The ESAs will also consider whether and how to account appropriately for Big Data related systemic risks in their risk assessments.

H. Role of regulators/supervisory authorities

69. The majority of respondents across the three sectors are of the view that the existing regulatory and supervisory framework is sufficient and that additional regulation regarding the use of Big Data by financial institutions is not needed. However, some respondents also noted that the implementation of Big Data technologies could benefit from further convergence and guidance in how these requirements are interpreted across Member States (for example, in relation to outsourcing rules) or how they apply in practice in the financial sector.

70. One stakeholder explicitly stated that in case certain risks materialise, the ESAs and European Institutions should not exclude regulatory or intervention measures. If additional regulatory measures were required, a wide group of stakeholders across the three sectors stated that they would prefer that such regulatory measures are technologically neutral and apply to all sectors equally.

71. Some respondents emphasised that Big Data was an opportunity for the financial sector and highlighted the importance of collaboration and support

from regulators and supervisors in order to help data drive innovations under a level playing field across the Single Market.

72. A few respondents also stated that the need for regulation should be treated cautiously, since Big Data is still in an incipient phase, and that the impact of differences in regulatory standards between the EU and the US should be taken into account, since Big Data is a global issue.

73. Respondents from the consumer side together with representatives from academia and the industry stated, however, that supervisory authorities should be able to detect and monitor emerging risks from the use of Big Data, including ESA/NCAs investigations on whether the use of certain types of data may act against the interests of consumers and whether the use of Big Data would require enhanced disclosures.

74. Some respondents also proposed that regulators need to have their own resources for Big Data supervision. The ability to review Big Data methodologies is required in order to limit consumer and competition detriment. A cross-sectoral range of respondents noted that Big Data would itself enable regulators to test other Big Data tools for shortcomings or the assessment of return and performance of certain investment products. Likewise, Big Data analysis tools could support Regtech and financial institutions in the provision of information to regulators.

ESAs' reactions

75. As already indicated, the ESAs will continue to closely monitor the use of Big Data across the three sectors and take further actions if and when required.

I. General comments on potential benefits and risks

76. The broad majority of respondents agreed with the ESAs description of potential benefits and risks for consumers and respectively financial institutions. Some specific comments were raised and are summarised below.

77. Some stakeholders provided examples of benefits observed in practice referring to inter alia faster responses to enquiries of customers and regulators or more efficient achievement of data storage obligations. A cross-sectoral range of respondents noted that some other benefits should be included, such as the potential of Big Data to test other Big Data tools for shortcomings, and, in the investment sector, the assessment of return and performance of long-term investment products.

78. Some stakeholders noted that consumer interaction would be improved only if financial institutions would share the data/algorithms with consumers and

if consumers have access to such Big Data tools, which is not typically the case.

79. Several respondents also noted that in order to pass on Big Data related cost-efficiency gains to consumers, effective competition, which is currently often lacking, would be required. Likewise, new costs, such as for comparison and guidance services or related to cyber security, data maintenance and HR, could offset potential cost-efficiency gains. In the same way, issues around appropriate access to data as well as new conflicts of interests, could hamper positive effects.

80. Some respondents however commented that some of the risks described in the Discussion Paper are neither caused nor exclusively linked to Big Data or only to the financial sector. Likewise, these risks could also stem from e.g. IT systems or the complexity of the financial system. Violations of requirements to act in the clients' best interests were rather conduct related, instead of being linked to the use of data driven technologies. Some respondents stated that the potential risks described in the Discussion Paper would only materialise if the existing regulatory framework (consumer protection, competition rules and financial rules) would not be applied and enforced properly. The majority of respondents stated that there is insufficient evidence on detrimental impact to justify additional regulatory intervention at the moment.

i. Potential impact on the implementation of product governance

81. A wide group of respondents (across the three sectors) agreed that Big Data could support the implementation of product governance, and oversight measures by helping manufacturers to better understand customer's needs and characteristics and to provide them with more targeted products adapted to consumers' needs and demands. Moreover, Big Data could support manufacturers in monitoring whether their products continue to be well suited to the consumers' interests, objectives and characteristics, as well as in the broader supervision of product governance requirements. This in turn could contribute to mitigate potential consumer detriment and conflicts of interest.

82. A few respondents, particularly from the banking sector, however believed that the applications of Big Data are in their infancy and therefore it is too early to tell how Big Data would impact product governance rules.

ii. Potential impact on the provision of advice on financial products to consumers

83. A majority of respondents believed that Big Data impacted positively the provision of advice to consumers, since it allowed for a more accurate and

consistent analysis of consumers` needs, at potentially more affordable prices.

84. However, other stakeholders had a different view, and pointed out the potential negative impact of Big Data on financial advice. Some respondents stated that Big Data based services/communications could raise risks for clients to consider and treat as advice other types of services or receiving advice without realising it is advice. The difference between targeted sales/guidance and provision of advice should be effectively enforced and disclosed to consumers. Some noted that advice at reduced price will be limited since Big Data applications require significant investments in IT and HR.

85. Moreover, certain respondents commented that the role of technology should be to support the provision of advice but that technology could not replace all human intervention/ face-to-face advisory services. Others stressed that the extent and quality of information provided by consumers would be important for the results of Big Data analytics. Therefore, regulatory guidance on techniques and methodologies on the risk-based models underlying the provision of advice would be welcomed.

86. However, several respondents noted that the GDPR rules on the use of personal data in the context of automated decision-making, or the MiFID II rules on advice and suitability statements, should adequately mitigate the risks.

iii. Potential impact on KYC processes

87. The majority of respondents across the three sectors agreed that Big Data has the potential of improving know-your-customer (KYC) processes and contribute to the detection of high-risk customers, money laundering risks and fraud more accurately. Respondents were also of the view that Big Data could reduce the costs of KYC checks.

88. However, the risk that financial service providers might collect consumer data with a commercial objective, using the AMLD requirements as a "smokescreen", was also mentioned.

iv. Potential impact on risk mitigation and prevention

89. Some respondents, particularly from the insurance sector, highlighted the beneficial impact of Big Data tools in the prevention and mitigation of risks. For example, the incipient use of telematics devices in insurance can help consumers be more aware of their exposure to certain risks and prevent such risks from materialising.

90. While acknowledging some of these benefits, some respondents from consumer organisations considered that the use of Big Data analytics in finance could be very intrusive in people's personal lives and start dictating not only where they drive but also how they eat, how many daily steps they need to take or even how they brush their teeth.

ESAs' reactions

91. The ESAs welcome the improvement that the use of Big Data techniques could bring on KYC processes and would like to remind that the AMLD strictly prohibits the processing of data collected in the context of this Directive for any other purposes, including commercial purposes.[12]

92. The ESAs also acknowledge the benefits of Big Data analytics in risk mitigation and prevention when it is done in compliance with the applicable legislations in place.

93. In addition, the ESAs will further assess, in each of their respective sectors, whether there is a need to monitor the impact of Big Data technologies on risk mitigation and prevention.

J. Potential non-regulatory barriers to the use of Big Data

94. A majority of respondents believes that certain non-regulatory barriers may interfere with the development and provision of Big Data tools. This includes the difficulty in changing the legacy IT technology of financial institutions, high investment costs (for example, to hire skilled IT staff or to manage/monitor the quality of data), or, third, the reputational risks associated with the use of Big Data, especially if based on processing consumer data or in case of security leaks.

95. In addition to the above barriers, respondents referred to other obstacles for the development and application of Big Data, such as poor quality of data, different standards for data formats, or consumers' attitude/willingness to have their data used.

K. Potential Additional existing legal requirements

96. Respondents across all three sectors generally agreed with the requirements listed in the section of the DP on the relevant regulatory framework.

12 Article 41(2) of AMLD.

97. Some respondents suggested, however a couple of further references to be added, for example in relation to copyright law, to Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, or to national professional secrecy rules, and the International Securities Services Associations Financial Crime Compliance Principles.

L. Potential development of Artificial Intelligence (AI) and Big Data

98. A number of respondents, especially in the securities sector, noted that the current level of development of AI technology is not mature enough to clearly predict how it could develop. However, a few stakeholders (including tech providers/Fintechs) believed that this technology has a lot of potential to instigate change, such as through the ability of analysing big volumes of unstructured and different data.

99. A majority of respondents saw AI as an additional layer of Big Data analytics and a key tool to improve discovering patterns on captured data, classification, evaluation and prediction. Certain stakeholders however also emphasized that AI would add to the complexity of Big Data tools, which could be more difficult to understand for financial institutions, users and supervisors.

5. Preliminary conclusions of the ESAs

A. Overview

100. The ESAs welcome the numerous and detailed comments received. The number of responses received[13] demonstrates the strong interest of stakeholders for this phenomenon.

101. The use of Big Data by financial institutions, like many technology related topics, represents an area where it is difficult to predict future developments accurately. Nevertheless, the responses received from stakeholders enable the ESAs to better understand the key expected benefits and risks of this innovation, as perceived by the market. It appears that most stakeholders agree that the use of Big Data has the potential to create numerous opportunities to offer consumers a better quality of products and services as well as benefits for financial institutions, provided that the key risks are adequately addressed.

102. As regards the need to address the risks identified in relation to this work, the ESAs note that some facets of the risks posed by the use of Big Data techniques are beyond the mandate of the ESAs even when such techniques are used by financial institutions. It actually seems that specific legislation in the field of data protection, cybersecurity and consumer protection is better positioned to address some of the risks identified in the context of this work.

103. As part of their ongoing monitoring of the use of Big Data in the financial sector, the ESAs will continue to engage on a regular basis with the data protection authorities and stand ready to support any initiatives by the data protection supervisors to provide guidance to the market on the applicability of the data protection requirements to Big Data applications in the financial sector.

104. The ESAs consequently decided to highlight in this Final Report some of the key responses brought by data protection, cybersecurity and consumer legislation to the challenges posed by the use of Big Data.

105. Nevertheless, the ESAs consider that for the time being the current sectoral financial legislation sets requirements that are capable to address a number of risks specific to the use of Big Data techniques by financial institutions. Indeed a number of existing far reaching requirements, while not designed with the risks posed by the use of Big Data in mind, are applicable irrespective of the technological context. The ESAs will continue monitoring the compliance with these existing legislative requirements and assess whether they effectively mitigate the risks identified. A selection of the key

13 68 Responses (public and confidential) were received in response to the Discussion Paper.

requirements deriving from financial sectorial requirements relevant in the context of the use of Big Data is laid down below. Furthermore, the ESAs consider that a legislative intervention at this point would be premature given that some key pieces of legislation, such as the GDPR or the new requirements under the PSD2, MIFID II or IDD, are still to be implemented or just entered into application.

106. The ESAs also consider it to be in the interest of financial institutions (notably taking into consideration the importance for them to build a long-term good reputation and trustful relationships) to develop and implement good practices promoting a fair, transparent and non-discriminatory treatment of consumers and ensuring that Big Data strategies remain fully aligned with the interests of consumers.

107. An indicative list of items that could be used by financial institutions to develop good practices in relation to the use of Big Data can be found below.

B. Requirements in the European data protection, cybersecurity and consumer protection legislation

108. As mentioned above, the ESAs consider that there are already a considerable number of legal requirements under the cross-sectoral legislation in the field of data protection[14], cybersecurity and consumer protection that aim to mitigate many of the risks identified in the context of this work and with which financial institutions must comply.

109. The ESAs believe it is relevant to highlight some of the key requirements in these areas relevant for financial institutions using Big Data techniques. For the avoidance of doubt, the ESAs wish to stress that the aim of this Report is not to provide an exhaustive overview of the applicable rules. The fact that certain other requirements are not highlighted in this Report does not mean that such requirements are not applicable for financial institutions using Big Data.

14 Sectorial financial legislations requires compliance with applicable data protection legislation. See Article 78 MiFID II, Article 104a UCITS, Article 37 IDD, Article 94 PSD2, Article 62 CRDIV.

i. Requirements in the field of Data Protection

- **General Data Protection Regulation (GDPR)[15]**

Purpose limitation

110. This criterion requires financial institutions to be able to justify the use of certain data categories as well as ensure the data is accurate and updated over time. This is done by defining a purpose for the collection of personal data and ensuring that any further processing is compatible with the original purpose.

Data accuracy and data minimisation

111. According to Article 5(1) of GDPR, data must be accurate and up-to date, adequate, relevant and not excessive in relation to the purposes for which they are processed. Further to these requirements financial institutions should be able to justify the use of certain data categories as well as ensure the data is accurate and updated over time. This consent must be freely given, specific, informed and unambiguous, and given a clear, affirmative action that shows the data-subject has given his/her consent.

Meaningful consent

112. According to Article 6(1) of GDPR, the processing of personal data must be carried out with the unambiguous consent[16] of the individual whose data is being used (the "data subject" or, for the purpose of this report, the consumer)[17].

113. While subject to a number of exceptions and exemptions, Article 9(2) of GDPR provides that this consent must be an explicit consent when the processing concerns personal data revealing for instance racial or ethnic origin, political opinions, religious or philosophical beliefs or data concerning health or sex life). According to Article 22(c) of GDPR explicit consent may also be needed for automated decision making[18].

114. It must however be mentioned that consent is not necessarily the only ground available for processing. Indeed, other processing grounds mentioned in Article 6(1) of GDPR include legitimate interest (article 6(1)(f) of GDPR), the necessity of the processing to comply with a legal obligation (article 6(1)(c) of GDPR) or the necessity for the performance of a contract concluded with the consumer (article 6(1)(b) of GDPR).

15 GDPR will enter into application on 25 May 2018.
16 Article 4(11) of GDPR.
17 Some exceptions are foreseen in GDPR.
18 For further information on profiling, please refer to "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" of 3 October 2017 (17/EN, WP 251) issued by the Article 29 Data Protection Working Party.

Right to Access to Data

115. According to Article 15 of GDPR, consumers have a right (i) to exercise the right of access to their data, in order to verify the accuracy of the data and the lawfulness of the processing, (ii) to request modifications or even (iii) to object to processing in certain circumstances.

116. According to Article 15 of GDPR, consumers should be informed in advance, if data about them is to be used in an automated decision making process, including profiling, and should be given information about the consequences of such processing.

Other Rights of Consumers

117. According to Article 22 of GDPR, consumers will also be able to (i) ask financial institutions that a human intervene in the profiling, to (ii) express their point of view and (iii) contest a decision based on profiling.

118. Consumers should also be given access to their "profiles" and to the logic of the decision-making that led to the development of their "profile" (this may imply for example the need for firms to explain how an algorithm reached a certain decision).

119. Also, GDPR gives consumers the right to request and receive the personal data that they have provided to a data controller and to transmit that data to another controller[19] (data portability).

Organisational and governance requirements

120. The protection of consumers' rights with regard to the processing of personal data also requires that appropriate technical and organisational measures are taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and to prevent any unauthorised access and processing.

121. Financial institutions are also expected under the GDPR to be able to demonstrate that they have taken the necessary steps to ensure compliance with the GDPR[20]. Among the measures that many firms may be required to take under the GDPR are the adoption of internal policies and measures that meet the principles of privacy by design and by default[21], the appointment of

19 Article 20 of GDPR.
20 E.g. Article 5 of GDPR.
21 Article 25 and Recital 78 of GDPR.

a data protection officer (DPO)[22] and the carrying out of data protection impact assessments[23].

- **E-Privacy Directive[24]**

122. The E-privacy Directive sets out rules to (i) ensure security in the processing of personal data, (ii) require notification of personal data breaches and (iii) guarantee confidentiality of communications[25]. The E-Privacy Directive[26] also provides that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user (e.g. cookies) is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

123. Article 13 of the E-Privacy Directive bans unsolicited communications where the consumer has not given its consent.

ii. Requirements under the Network and Information Systems Directive (NIS)[27]

124. According to Article 14 of the NIS Directive operators of essential services (e.g. credit institutions, financial market infrastructures) have to take appropriate security measures to manage the risks posed to the security of networks and information systems which they use in their operations and to notify serious incidents to the relevant national authority[28].

iii. Requirements in the field of Consumer Protection

- **Unfair commercial practices Directive (UCPD)[29]**

125. Article 5 of the UCPD prohibits unfair commercial practices which are contrary to the requirements of professional diligence and are likely to distort the economic behaviour of the consumer.

126. According to Article 5(4) of the UCPD, (i) misleading actions or (ii) omissions as well as (iii) aggressive practice, including making persistent and unwanted

22 Articles 37 – 39 of GDPR.
23 Article 35 of GDPR.
24 Directive (EC) 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
25 The rules may provide various protections concerning the use of cookies or similar technologies to store information or access stored information on a user's device.
26 Article 5(3) of E-Privacy Directive.
27 Directive 2016/1148 on Security of Network and Information Systems.
28 See also EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP): Available here.
29 Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices.

solicitations by telephone, e-mail or other media constitutes unfair commercial practices.

- **Directive on Distance Marketing of Financial Services**[30]

127. Articles 9 and 10 of the Directive on Distance Marketing of Financial Services ban abusive marketing practices seeking to oblige consumers to buy a service they have not solicited.

C. Requirements under the sectorial financial legislation

128. Sectoral financial legislation aims at remaining technology neutral[31]. The European legislators intend to ensure that financial institutions undertaking the same activity are subject to the same set of requirements irrespective of the means through which the service is delivered. This approach aims at preserving a level playing field among financial institutions while enabling technological innovation.

129. This neutrality towards the technology used by financial institutions to service customers does not mean that financial legislation is not intended to apply to the use of technological tools such as Big Data techniques by financial institutions. Sectoral financial legislation applies to the use of Big Data by financial institutions.

130. Furthermore, the ESAs consider that some of the provisions contained in the sectoral financial legislation are particularly relevant to tackle some of the risks identified in relation to the use of Big Data techniques by financial institutions. This sub-section lists these requirements. The list below is not intended to be an exhaustive list of requirements[32].

i. Organisational and prudential requirements

131. The ESAs stress the relevance in the Big Data context of the provisions requiring financial institutions to:

a. **Establish and operate sound internal control mechanisms, effective procedures for risk assessment and effective control and safeguard arrangements for information processing systems**[33].

30 Directive 2002/65/EC on distance marketing of consumer financial services.
31 See European Commission Consultation Paper, "Fintech: a more competitive and innovative European financial sector" 23 Mars 2017.
32 This list refers mostly to legislative acts that already entered into force in the EU, although some of them are yet to be implemented by Member States at the date of publication of this report.
33 See Article 16(5) MiFID II, Article 18 AIFMD and Article 12 UCITS, Articles 5 and 95 of PSD2. See also Articles 41, 44 and 46 of Solvency II requiring all insurance and reinsurance undertakings to have in place an effective

These requirements are of utmost importance for business processes using Big Data technologies. They notably require financial institutions using Big Data technologies to allocate appropriate capital, human and IT resources to the implementation of Big Data from an operational standpoint.

b. **Ensure continuity and regularity in the performance of their activities** (and employing appropriate and proportionate systems, resources and procedures to this end) [34].

Complying with these provisions is important in order to mitigate any challenges or risks resulting from the implementation of Big Data processes. These provisions also require financial institutions to factor the possible threats that may impact the continuity and the regularity of the performance of the financial institutions' activity.

c. **Monitor markets activity, mitigating against counterparty or systemic risk or disorderly trading**[35].

Investment firms and trading venues are subjected to such provisions in order to ensure that robust measures are in place to avoid that algorithmic trading or high-frequency trading disrupt the markets.

d. **Ensure that any reliance on a third party (i.e. outsourcing) does not impair the quality and the continuous performance of services**[36].

132. The ESAs note that the use of Big Data technologies and applications is an area where financial institutions are particularly likely to consider outsourcing to third-party providers, such as data-vendors or cloud computing service providers. In this respect, the ESAs wish to stress that sectorial legislation requirements applicable to the outsourcing of important functions of financial institutions do apply when an external provider is performing all or part of the outsourced functions through the use of Big Data technologies.

In this respect, the ESAs stress that (i) financial institutions are required to take appropriate arrangements to mitigate the risks related to the use of third-party service providers in accordance with applicable sectoral legislation, (ii) that the outsourcing should not impair the quality of financial institutions' internal control and the ability of the competent authorities to

system of governance which provides for sound and prudent management of the business. Article 88 of CRD IV also establishes general obligations related to governance arrangements, adequate internal control mechanisms that are consistent with and promote sound and effective risk management. In addition to this, in the payments field, the PSD2 and the level-two legislation that the EBA has been mandated to develop in support of the PSD2 provide a number of requirements regarding the management of operational and security risks, that will apply to all credit institutions, payment institutions and e-money institutions.

34 See Article 16(4) and 17 of MiFID II, Articles 5 and 95 of PSD 2, Article 41 Solvency II.

35 See Article 17 of MiFID II, Article 79 of CRD.

36 See Article 16 of MiFID II, Article 13 of UCITS, Article 19(6) of PSD II, Articles 38 and 49 of Solvency II.

monitor the financial institution's compliance with all its obligations, and (iii) that financial institutions remain fully responsible for discharging all their obligations under relevant sectorial legislation (even when several third-party providers are involved).

e. **Comply with record-keeping requirements**[37]

The ESAs also want to stress the importance of compliance with applicable sectoral requirements in the field of record-keeping and any other regulatory audit trail requirements of the decision-making of financial institutions and confirm that these requirements apply when such decision making process is performed totally or partially using Big Data techniques or applications. As mandated in sectoral legislation, this information should be made available to the competent authorities upon request.

The ESAs consider these requirements to be key in the Big Data context as they enable to reconstruct efficiently and evaluate the Big Data strategies/tools employed and ascertain compliance of financial institutions with all applicable regulatory requirements when providing services to consumers.

f. **Take steps to identify, prevent and manage conflicts of interests**[38]

The use of Big Data can generate new contexts involving conflicts of interests, for instance from embedded biases or flaws in Big Data tools favoring firm's interests or certain clients over other clients.

ii. Conduct of business requirements

133. The ESAs stress the relevance in the Big Data context of the conduct of business principles requiring financial institutions to:

a. **Act honestly, fairly and professionally**[39].

Financial institutions, to the extent that they are subjected to sectoral legislation requiring them to act honestly, fairly and professionally, should carefully consider these far reaching principles when setting-up procedures and methodologies using Big Data technologies. Financial institutions should notably set-up procedures aiming at promoting fair and non-discriminatory

37 See Articles 13(6) and 17 MiFID I; see also new Article 17 MiFID II concerning algorithmic strategies. See also Article 258(1)(i) of Solvency II Delegated Regulation (EU) 2015/35, of 10 October 2014. See also in the banking sector the Guidelines on outsourcing issued in December 2006 by the Committee of European Banking Supervisors (CEBS) (available here) and the more recent Final Report of recommendations on outsourcing to cloud service providers published by the EBA in December 2017 (available here).
38 Art. 18 MiFID I (Art 23 MiFID II), Art 17, 27 and 28 IDD, Art 7of MCD. See also Article 258(5) of Solvency II Delegated Regulation (EU) 2015/35, of 10 October 2014. See also EBA Guidelines on product oversight and governance arrangements for retail banking products July 2015 (available here).
39 See Article 24(1) of MIFID II, Article 17(1) of IDD, Article 7(1) of MCD, Article 12 of AIFMD, Article 14 of UCITS.

practices. The requirement to act fairly is of particular importance when the procedure or methodology being set-up or up-dated consists in the profiling of consumers through means enabled by Big Data.

b. **Manufacture and distribute products and services which meet the needs of identified target clients and monitor such products**[40];

Financial institutions should factor and monitor the potential impact of the use of Big Data tools and techniques in the context of the application of their product oversight and governance processes. Notably, they should ensure that the use of Big Data tools to (i) identify target markets or (ii) assign a customer to a target market, is compliant with applicable legal requirements. Financial institutions should specifically scrutinize that the services and products distributed are compatible with the needs and characteristics of the identified target market and, when applicable, monitor such products.

c. **Ensure that all information, including marketing communications, addressed by financial institutions to customers are fair, clear and not misleading**[41].

These requirements apply when financial institutions use Big Data technology to launch targeted marketing and communication campaigns.

d. **Assess certain minimum, accurate and up-to-date, information about clients and products/services before providing certain services** (e.g. suitability or appropriateness tests or creditworthiness assessments)[42].

e. **Preserve the interests of consumers when purchasing bundled or tied packages of products** (in particular, client mobility and ability to make informed choices at the right time in the sales process)[43].

These provisions should prevent firms from using Big Data in order to promote bundled or tied packages of products which are not in the interests of clients.

f. **Establish fair and efficient claims and complaints handling processes**[44].

40 Articles 16(3) and 24(2) MiFID II, Article 25 IDD, EBA Guidelines on product oversight and governance requirements for manufactures and distributors of retail banking products, July 2015.
41 See Article 16 of MiFID II, Article 13 of UCITS, Article 19(6) of PSD II.
42 See Article 25 of MiFID II, Article 30 of IDD, Articles 18 and 20 of MCD.
43 See Article 24(11) MiFID II, Article 24 IDD, Article 12 MCD, Article 9 PAD, Articles 66 and 67 of PSD2
44 See for instance Article 14 IDD; Article 26 in the MiFID II Delegated Regulation requires firms to establish, implement and maintain effective and transparent procedures for the prompt handling of complaints, and article 101 PSD2, under which payment service providers should put in place and apply adequate and effective complaint

This requirement is relevant to ensuring that Big Data analytics (e.g. tools enabling to predict more accurately whether a given consumer is likely or not to lodge a claim/complaint) do not lead to consumer detriment.

D. Good practices for financial institutions using Big Data

134. As mentioned above, the ESAs acknowledge that the use of Big Data technologies can be beneficial for financial institutions and consumers alike, as well as for the market of financial services and products as a whole. However, the use of Big Data also poses a number of significant risks which have the potential to prevent such benefits from materialising and could damage the trust of consumers in financial institutions.

135. The use of Big Data technologies is, like any technology-based phenomenon, expected to evolve in the years to come in a number of possible, yet unpredictable, ways. This continuous evolution is an additional layer of difficulty to the role of legislators and supervisors.

136. In order to address such a fast-evolving phenomenon, the ESAs believe it is relevant to promote not only the strict compliance with applicable requirements but also the development and adherence by financial institutions to good practices promoting a fair, transparent and non-discriminatory treatment of consumers, when using Big Data-based technologies.

137. The adherence to such good practices, combined with the compliance with applicable data protection, consumer protection and financial legislation requirements, could contribute to ensuring that Big Data strategies are designed in a responsible way and take into account consumers' interests.

138. The ESAs suggest below an indicative a list of arrangements and behaviours that could be followed by financial institutions to develop good practices on the use of Big Data

Robust Big Data processes and algorithms

a. The periodical monitoring of the functioning of Big Data procedures and methodologies as well as Big Data tools to adapt to technological developments and newly emerging risks.

resolution procedures for the settlement of complaints of payment service users. See also the Joint Committee Final Report on guidelines for complaints-handling for the securities (ESMA) and banking (EBA) sectors (available here).

Consumer protection

b. The periodical assessment whether Big Data based products and services are aligned with consumers' interests and where relevant, the review and adjustment of the Big Data tools.

c. The setting-up of procedures aimed at taking appropriate remedial actions when issues that may lead to consumer detriment materialise or are anticipated (notably in relation to the segmentation of consumers, e.g. impact on pricing or access of consumers to services due to increased segmentation of the target market).

d. Factor the potential risks associated with the use of Big Data together with the content of the financial institution's Big Data transparency policy when designing and enforcing the financial institution's complaint handling framework.

e. The adherence to and strict compliance with industry-specific codes of conduct under the GDPR[45].

f. Pay special attention to their policy in terms of processing of data gathered from social media platforms considering the varied level of understanding by consumers of privacy settings on social media accounts[46] and the risks of inaccuracies in such data.

g. Strive to maintain a balance between automated decision-making tools and human interventions.

Disclosure on the use of Big Data

h. Ensure a high level of transparency towards customers concerning the use of Big Data technologies to process their data.

i. Contribute to the promotion of public awareness, consumer education on the phenomenon of big data and of consumers rights related to the use of Big Data by financial institutions.

45 Pursuant to GDPR, financial institutions may choose to voluntarily join and adhere to approved codes of conduct or approved certification mechanisms, as an element to demonstrate compliance with GDPR (see Articles 24(3), 28(5) and 40-43 of the GDPR).

46 Data protection bodies have explicitly referred to these risks and advised financial institutions to consider whether they have legitimate grounds to use data that may have been gathered from social media platforms or other online sources for insurance purposes, rather than merely relying on the fact that some content is accessible. e.g. UK Information Commissioner's response to the Financial Conduct Authority's call for inputs on big data in retail general insurance (8 January 2016).