CRO INSIGHTS JOURNAL

GETTING READY FOR THE NEW GENERAL DATA PROTECTION REGULATION
In the past year, mankind produced as much data as in all of its previous history, and most data is generated by consumers. Walmart alone handles a million customer transactions an hour, feeding databases with more data than the equivalent of all the existing books in the world.

20 years after the Data Protection Directive and after five years of debate, the EU General Data Protection Regulation was passed in 2016 and will apply from 25 May 2018. It dramatically overhauls personal data protection rules, imposing significant penalties for violations – possibly up to 4% of an organisation’s annual global turnover.

There have been vast changes since the 1995 introduction of the Directive that is being replaced – only 1% of the European population was using the internet then. The GDPR governs the processing of personal data – factors specific to the physical, physiological, genetic, mental, economic, cultural, social or biometric identity of a person. It covers concepts including territorial scope, consent, breach notification, access, the ‘right to be forgotten’, portability, privacy by design, data protection officers and pseudonymisation.

In this edition, we set up the scene with our friends from the Liedekerke law firm (Etienne Kairis, Erika Ellyne and Dorien Taeymans).

We then enter the discussion of how the GDPR is being handled by banks (Olivier Goffard, Euroclear Group and Lucas Quarta, BNP Paribas Personal Investors), and we can see that the lessons learned apply to all. We list the challenges and give recommendations (Dean Mitchell, and Magali Caroline van Coppenolle, Avantage Reply).

We finally welcome you to put yourself in the shoes of a DPO and tackle the complexity of GDPR with a Privacy Asset Inventory (Alberto Canadè, Spike Reply).

I hope you find this edition of the Journal insightful, and we look forward to further conversations with you.

---

Freddy Gielen
Executive Partner
Avantage Reply

---

3 The Economist, "Data, data everywhere", 25 February 2010; The Telegraph, "Google counts total number of books in the world", Hunter Skipworth, 6 August 2010.
The European Commission has introduced the General Data Protection Regulation which will become effective from 25th May, 2018. The Regulation has been implemented in order to:

- Force companies to be clearer on their data collection and use;
- Improve data protection and prevent data infringement;
- Establish improved control and reactivity to prevent data leakage.
| CONTENTS |
|-----------------|--------|
| **Overview of the EU General Data Protection Regulation** | 4 |
| **GDPR: A new Data Protection Landscape for Bankers** | 10 |
| Olivier Goffard, Head Of Group Compliance & Ethics at Euroclear Group | |
| Lucas Quarta, Chief Data Officer, BNP Paribas Personal Investors | |
| **Implementing GDPR: Challenges and Recommendations** | 16 |
| **Reply Privacy Asset Inventory: Tackling GDPR challenges in an era of deep Digital Transformation** | 30 |
Olivier Goffard is Head of Group Compliance & Ethics at Euroclear Group. Olivier has spent more than 16 years in the banking sector and is supervising a team of more than 50 professionals in Europe, Hong Kong and the United States. He is a talented and experienced Compliance & Ethics professional combining legal and audit background. Olivier holds a Master in Company Law from the University of Ghent (Belgium). He is certified from the Association of Certified Anti Money Laundering Specialists (ACAMS).

Etienne Kairis has over 18 years of experience in commercial law and technology, with a focus on IT law, data protection, intellectual property rights, fair trade practices and distribution (in particular in the automotive sector). Etienne has developed expertise as regards the regulation, organisation, and effective management of large scale data for a variety of different actors (public and private sector, large and small entities). Moreover, Etienne regularly advises clients with respect to their internet presence and activities as well as software matters both of a transactional and litigious nature. He has further gained broad experience in devising and enforcing national and international strategies for intellectual property protection (trade mark, patent and copyright protection).

Erika Ellyne is Junior Associate at Liedekerke Wolters Waelbroeck Kirkpatrick. She graduated from the University of Brussels (ULB 2008) and then proceeded to complete an LL.M in European and International Law (VUB 2009). Thereafter, she remained at the VUB as a researcher, at the heart of the Law, Science, Technology and Society Studies (LSTS) research center. LSTS organises every year the Conference on Computers, Privacy, and Data Protection. During her time as a researcher, Erika’s work focused on data protection and intellectual property. Furthermore, she received the BAEF fellowship to conduct research for a year at the University of Wisconsin-Madison. Erika joined the bar in 2015. The practice she works in remains focused on data protection, IT matters, and intellectual property.

Lucas Quarta has a PhD in Mathematics. He was Head of IT ALM & Treasury and Basel III Program Director for BNPP Fortis until mid-2012 when he became the Program Director for a huge BNPP Group wide Securities Handling program until mid-2015. Between mid-2015 until the end of 2016 Lucas was the Data Management Program Director for BNP Paribas Domestic Markets entities and since the beginning of 2017 he holds the position of Chief Data & Analytics Officer of BNP Paribas Personal Investors.

Dorien Taeymans graduated as a Master in Law from the University of Antwerp (UA 2013). During her education, she studied at Stellenbosch University in South Africa. In addition, she followed an internship at the permanent mission of Belgium to the United Nations in New York and is currently following an Advanced Master of Intellectual Property and ICT Law at the University of Leuven (KULeuven).

Dorien’s practice is focused on data protection, IT matters, and intellectual property. She carries out data audits and advises clients on privacy policies and GDPR compliance strategies. Dorien is a member of the Brussels Bar since 2015 and joined Liedekerke Wolters Waelbroeck Kirkpatrick in 2015.

Olivier Goffard is Head of Group Compliance & Ethics at Euroclear Group. Olivier has spent more than 16 years in the banking sector and is supervising a team of more than 50 professionals in Europe, Hong Kong and the United States. He is a talented and experienced Compliance & Ethics professional combining legal and audit background. Olivier holds a Master in Company Law from the University of Ghent (Belgium). He is certified from the Association of Certified Anti Money Laundering Specialists (ACAMS).
Freddy Gielen is a Founding Partner of Avantage Reply and responsible for the firm's activities across EMEA. Freddy is a specialist in finance and risk within 20 years of financial services experience. He started his career in Luxembourg with Arthur Andersen and developed his experience further as a Senior Manager with Ernst & Young in Asia and the United States before spending five years with The World Bank Group working on financial sector regulation in Europe and the United States. Freddy is a Réviseur d’Entreprises (Luxembourg) and a U.S. Certified Public Accountant (CPA). Until 2010, he was a member of a working group advising the International Accounting Standards Board (IASB) and he co-chaired the Accounting and Auditing Practices Committee of the International Corporate Governance Network (ICGN).

Dean Mitchell is Associate Partner at Avantage Reply UK. He has over 25 years of international banking and financial services experience across Canadian, British and European markets. During this time Dean has gained an excellent insight and first-hand experience of the challenges financial institutions face in adapting to market changes and executing business process changes. Prior to beginning his consulting career in 2009, Dean worked in a number of executive roles in Europe and the UK including, CRO of a mid-size Dutch Bank, Director of Risk for the Mergers & Acquisition practice of GE Capital Europe, and Joint Director of Credit Risk for all of GE’s Joint ventures in Europe.

Magali Caroline Van Coppenolle is a Senior Consultant with Avantage Reply UK. She combines an in-depth understanding of regulatory frameworks with experience in strategy to support clients’ change delivery. Magali has previously worked with regulators on behalf of the World Bank. She has led change management teams on implementation and supervision projects. During her degree, Magali completed a research project on counter-cyclical capital ratios with the Bank of England before jointly graduating from the Hertie School of Governance, Berlin, and the London School of Economics.

Alberto Canadè is DPO at Reply in Italy. In 2001, after a short experience in the Telco market (in both Italy and France) as Software Test Manager, he started his career in ICT Security at Elsag Datamat, Finmeccanica Group. Prior to this current role and since 2008, he joined Spike Reply, the Reply Company specialising in Cyber security, Risk Management & Compliance, and System Integration, as Manager in the Risk Management & Compliance practice. Alberto obtained four different IAPP certifications on privacy (CIPP/E, CIPP/US, CIPT and CIPM), all currently valid.
OVERVIEW OF THE EU GENERAL DATA PROTECTION REGULATION

WHAT YOU NEED TO KNOW ABOUT THE GDPR

It took four years of hard-fought negotiations but, in 2016, the European Union’s Regulation on data protection (‘GDPR’) finally saw the day. The GDPR replaces the previous 95/46/EC Directive (‘the Directive’). The GDPR’s provisions will only effectively apply as from 25th of May 2018, allowing sufficient time for companies to adopt compliance measures. In an increasingly data driven society, the main objective of the GDPR is to offer EU-wide comprehensive privacy and data protection safeguards to all European citizens. This article provides an overview of the key elements you should know about the GDPR.

EXPANDED TERRITORIAL REACH

The GDPR’s territorial scope of application has been considerably widened as compared to the Directive. Pursuant to its Article 3, the GDPR applies to all entities operating in the EU, regardless of the location of their data controller and/or processor. The scope of application is further detailed below.

Firstly, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU, regardless of the actual location of such processing. Note that the broad interpretation the Court of Justice of the European Union (‘CJEU’) gives to the concept of ‘processing personal data in the context of the activities of an establishment’ under the Directive will still be relevant under the GDPR.

Secondly, and perhaps more importantly, entities established outside of the EU fall under the scope of the GDPR whenever they process personal data of data subjects that are in Europe.
In this respect, the types of processing activities that trigger the GDPR’s application are the offering of goods or services to the data subjects (whether paid or not), or by monitoring their behaviour.

Lastly, the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law, irrespective of a data subject’s location.

Importantly, entities subject to the GDPR’s jurisdictional reach that are established outside the EU must appoint an EU based representative.

THE PRINCIPLES OF DATA PROTECTION AND AN UPDATED NOTION OF CONSENT

The cardinal principles of personal data processing, while updated, remain, by and large, unchanged. As a brief reminder, processing of personal data must follow the principles of: fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security, integrity and confidentiality. Those principles are restated in Article 5 of the GDPR. Hereafter, we focus on what we believe is a most noteworthy modification made under the GDPR: the interpretation of consent, which may be one of the most – if not the most – prevalent legal bases used by controllers in practice.

For the processing of personal data to be lawful, it must satisfy the conditions set out by Article 6(1) of the GDPR, which for the most part, replicates identical grounds to those found in the Directive. Article 4(11) of the GDPR defines ‘consent’ as any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. With this definition, the GDPR adopts a more restrictive approach to ‘consent’ than the Directive. In particular, it seeks to ensure that consent is specific to distinct purposes or processing.

A further addition to the definition of consent is the need for an ‘unambiguous indication’ of the data subject’s agreement to the processing of their personal data. This can be indicated by a written, including electronic means, or an oral statement or action. Pursuant to Recital 32 of the GDPR, this covers ticking a box when visiting an internet website, choosing technical
settings for information society services another statement or conduct which clearly indicates in [the] context, the data subject's acceptance of the proposed processing [...]. Recital 32 further specifies that silence, pre-ticked boxes or inactivity do not, therefore, constitute consent.

Article 7 further specifies conditions for consent to be 'valid'. For example, when part of a broader written declaration, it must be distinguishable from other matters within the declaration, it must be revocable at all times and it should not be made contingent to the provision of a contract if it is not necessary for the performance of that contract.

Finally, special cases exist. The processing of 'sensitive data', such as racial or ethnic origins, political opinions, religious or philosophical beliefs or sexual orientation, is strictly conditioned as per Recital 51 and consent must be explicitly provided. Article 8 of the GDPR also sets out specific conditions for the consent of children.

NEW RIGHTS FOR DATA SUBJECTS

The GDPR strengthens rights already granted under the Directive, such as the right of access, the right of rectification, the right to object and the right to non-automated individual decision-making. It also includes an additional layer of protection for data subjects under the form of new rights. These new rights, listed below, will have to be implemented and enforced by controllers and processors in their daily business activities.

■ Right to information and access (Article 12-15 of the GDPR): the scope of the information to be provided by the controller to the data subject when collecting the latter's personal data is broadened. Furthermore, upon the request of data subjects, controllers have a new obligation to provide them with a copy of their personal data being processed;

■ Right to erasure (Article 17 of the GDPR), also known as the “right to be forgotten”: under certain circumstances, among others when the data is no longer necessary, when consent has been withdrawn or when the data has been unlawfully processed, the controller is under the obligation to erase the personal data he or she has been or is processing;

■ Right to restriction of processing (Article 18 of the GDPR): under specific circumstances, such as contesting the accuracy of personal data or questioning the lawfulness of the processing, data subjects have the right to request the restriction of processing by the controller. In which case, the processing should be limited to data storage only;

■ Right to data portability (Article 20 of the GDPR): if personal data processing is done automatically and has been consented to or is necessary for the fulfilment of a contract, the data subject can request that the controller transmit the personal data directly to another controller, in a machine-readable format.

DATA GOVERNANCE OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

The GDPR imposes new and more constraining obligations on both controllers and processors of personal data. Indeed, and in contrast with the Directive, data processors are in the frontline as they are now held directly
liable with regard to the enforcement of data protection regulations.

**Key obligations for both controllers and processors include, among others:**

- **Privacy by design and default** (Articles 24-29 of the GDPR): when determining the means by which the personal data are to be processed, namely technology solutions and process design, some features must be integrated “by default”. This includes, for example, data minimisation: the principle that only personal data that are strictly necessary for a specific purpose are processed. Other examples of measures include pseudonymisation or the adoption of appropriate internal policies. Beyond the implementation of appropriate technical and organisational measures to allow for the lawful processing of personal data, processors and controllers must also be able to demonstrate that processing is performed in accordance with the GDPR.

- **Keep a record of processing activities** (Article 30 of the GDPR): this obligation replaces the Directive’s requirement to notify or seek approval from the National Data Protection Authority (‘DPA’) in certain circumstances. Under the GDPR, organisations with more than 250 employees will have to maintain a record of processing activities conducted under their responsibility. This record must contain specific information, such as, and among others, contact details, processing purpose;

- **Appoint a Data Protection Officer** (Article 37-39 of the GDPR): organisations can, and in certain cases must, appoint a DPO. Organisations for which it is compulsory include: public authorities, companies with processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale as their core activities and companies mainly processing sensitive data on a large scale, such as hospitals;

- **Data breach notification** (Article 33-34 of the GDPR): processors must notify controllers of a personal data breach, without undue delay. In turn, controllers are required to notify such breach to the regulatory authorities, no later than 72 hours after becoming aware of the breach. In case the data breach is considered to bear a high risk to the “rights and freedoms of natural persons”, the controller may be under the obligation to notify the data subjects concerned by the breach.

**Specific obligations for controllers**

- **Data Protection Impact Assessments (‘DPIAs’)** (Article 35 of the GDPR): controllers have the obligation to conduct DPIAs on any processing activity that is considered ‘high risk’ prior to the start of such activities. Whether or not such high risk exists is measured by reference to the risk of infringing a natural person’s rights and freedoms. The objective of such DPA is to investigate the appropriate technical and organisational measures to be taken to guarantee a security level in line with the risks identified;

- **Conclude written agreements** (Article 26 and 28 of the GDPR): based on already existing provisions in the Directive, whenever controllers and/or processors work together, they must conclude written agreements that contain specific obligations and liability clauses.
OVERVIEW OF THE EU GENERAL DATA PROTECTION REGULATION

ENFORCEMENT

Enforcement is a key issue for businesses, helping them shape compliance measures and response. Regulatory bodies have an important influence on how and when regulations are enforced, and it may be critical for businesses to know more about the regulatory bodies under the new GDPR regime.

National Data Protection Authorities

The National Data Protection Authorities, also known as DPA not only keep their function and competences, as defined under the Directive, but are also given greater powers under the GDPR. DPA will now be able to impose significant administrative fines on data controllers and processors. The GDPR establishes a tiered approach to penalties for breach, which allows the DPA to impose fines up to 10 million Euros or 2% of global turnover, depending on what indicator is the highest. In other circumstances, DPA may also be able to impose fines, worth up to double the value defined in the first tier.

Moreover, the burden of proof is now reversed as, in the event of doubt of whether or not the organisation complies with the GDPR, the entity bears the burden to prove its compliance, as per the newly defined Accountability principle under the GDPR.

European Data Protection Board

The GDPR introduces the EDPB, a new EU body with extensive powers that replaces the old Article 29 Working Party. It is comprised of the EU’s national supervisory authorities, the European Data Protection Supervisor and the EU Commission. The role of the EDPB is to settle disputes between national supervisory authorities, to provide advice and guidance, as well as to approve EU-wide codes and certification.

Complete Harmonisation?

It is worth mentioning that although one could expect that the GDPR would achieve a full harmonisation of the data protection landscape in the EU, there is still some room left for national legislators to adopt national rules in various areas, such as data processing in an employment context, data processing for scientific, historical or statistical purposes, and so forth. This will be important, and potentially burdensome, for international organisations active in different EU jurisdictions, as they will still have to monitor the different national legislative initiatives in the field of data protection.

---

4 See GDPR recital 22 “Establishment implies the effective and real exercise of activity through stable arrangements.”
5 E.g. CJEU 1 October 2015, Weltimm, C-230/14; CJEU 13 May 2014, Google Spain v Gonzalez, C-131/12; CJEU 28 July 2016, Verein v Amazon, C-191/15.
6 It follows from Recital 23 of the GDPR that the mere accessibility of a website is not enough; a certain degree of targeting is required depending on e.g. the language used, the currencies available to conduct your purchase and nationality of the customers who have written reviews. The decisions of the CJEU regarding “directed to” EU member states in the context of the Brussels Ibis Regulation (1215/2012/EC) are likely to aid interpretation under this similar aspect of the GDPR (e.g. CJEU 7 December 2010, Pammer and Hotel Alpenhof, C-585/08 and C-144/09).
7 Internet use profiling by tracking of individual’s behaviour online is expressly referred to as an example of monitoring in recital 24 of the GDPR.
8 See GDPR recital 25: “Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State’s diplomatic mission or consular post.”
9 Article 7 Directive 95/46/EC: (a) consent; (b) necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) necessary for compliance with a legal obligation to which the controller is subject; (d) necessary in order to protect the vital interests of the data subject or of another natural person; (e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) the legitimate interests pursued by the controller or by a third party.
10 Recital 32 GDPR states “When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”
11 Recital 51 GDPR.
12 Article 6.1.(a) and Article 9.2.(a) GDPR.
13 Article 6.1.(b) GDPR.
14 For more examples see recital 78 and article 32 GDPR.
15 Please note that when organisations chose to do so they must adhere to the obligations under the GDPR regarding the appointment of such DPO as well as the organisation of his tasks.
OVERVIEW OF THE EU GENERAL DATA PROTECTION REGULATION
OLIVIER, DO YOU BELIEVE THAT GDPR WILL SIGNIFICANTLY IMPACT YOUR ROLE AT EUROCLEAR?

Definitely, there will be an impact. Can we consider this impact as significant? I am less convinced if we compare ourselves to that of the retail sector, but of course this new Regulation requires a heavy investment of resources and energy to be compliant by the due date.

The impact is probably less for us, not only because we are in a mainly B2B environment but also because we have always considered data privacy to be important and, therefore, we already have a DPO and a comprehensive policy and procedure framework. Also, data privacy is, of course, already part of our periodic Compliance Risk Assessment. Nevertheless, it will require much more work with respect to the accountability principle, as described in the GDPR, and the consequent need for more documentation and formalisation, and this is without even mentioning the impact on the IT systems.

In addition, there are new elements like Privacy by Design and the data register that we will have to integrate into our governance framework.

This is not only about the creation of a new Data Governance Framework, it is also a matter of maintaining momentum in our compliance efforts. This will require additional resources on a continuous basis. Even if we have already updated our data register once, this needs to
happen on a regular basis in order to be of added value. So, to make a long story short, we have a good basis to start with and we are capitalising on that, but the impact on us remains significant.

**DO YOU BELIEVE THAT GDPR IS ALSO PROVIDING YOUR COMPANY WITH OPPORTUNITIES?**

I do not see any direct business opportunities linked to the implementation of GDPR. But, of course, indirectly, it could have some positive side effects. The GDPR implementation project could positively increase compliance awareness inside the organisation. **This project is being discussed and implemented through the Board of Directors, the management and the whole organisation. This provides a real opportunity to increase our firm's overall compliance awareness and further improve our excellence in compliance.** Also, let's face it, the big fines announced everywhere in the press have put personal data protection on the Board's agenda, even if DPA's will only use those fines in exceptional cases. Regarding data governance and GDPR, the overlaps are obvious, but, until now, we are managing GDPR and Data Governance separately. It is hence quite difficult to say if the GDPR implementation will enable us to limit the amount of data that we store or the retention period.

**WHAT ARE THE BIGGEST CHALLENGES FOR A PRAGMATIC IMPLEMENTATION OF THE GDPR?**

The GDPR is a broad and complex Regulation. Therefore a risk-based approach is key. A very good knowledge of the firm's risk profile is essential. I strongly believe that a deep understanding of the risks linked to the GDPR is key to achieve an astute implementation of the GDPR. It is important to clearly identify the most important risks and to allocate resources wisely. This good understanding will provide us with a solid foundation to be able to mitigate risks efficiently as well as to demonstrate to the Regulators that we have defined the right approach for compliance. Indeed, for certain risks, we will implement solutions immediately, but more efficient solutions may be implemented after May 2018, as they may require refinement and additional resources and budget. Nevertheless, on D-Day, we will be able to demonstrate that we take the GDPR seriously. The implementation of the new data subjects' rights, the identification of sensitive data, the performance of DPIA where relevant and the implementation of the privacy by design are considered to be priorities, which have not been as yet regulated in this way before the introduction of the GDPR.

**HOW WILL THE GDPR IMPACT YOUR ORGANISATION IN THE SHORT AND LONG RUN?**

If we assess only the financial impact then, without a doubt, there will be a negative impact. The implementation costs in the short term and in the longer term due to the ongoing maintenance cost such as implementing the privacy by design will increase our operational costs. The new regulations should be considered as justified and once implemented will lead to an improvement of our data privacy management. Therefore, if we broaden the scope of the impact to non-financial aspects, I believe that we can leverage on the GDPR implementation project to increase compliance awareness and improve Data Governance, including data lifecycle aspects. We also believe that it is a unique opportunity to re-consider data management practices and processes beyond the data processes related to the GDPR.
WILL GDPR IMPACT YOUR BUSINESS ORGANISATION? WHAT WILL BE THE STRENGTH OF THE IMPACT?

Euroclear has a very specific business model, and hence, there will of course be an impact across the whole organisation as well as on HR because of the nature of the data processed for their core activities. With regard to marketing, the impact should be limited as we do not use profiling for our business development. Overall, I expect the largest impact on the organisation in the areas of compliance and IT, especially with regard to the privacy by design and the automation of our proposed solutions.

WHAT IS THE MAIN MESSAGE YOU WANT TO GET THROUGH?

My main message would be to not focus on the potential fines. Of course, potential fines might be higher but what should be very important for each employee is to do the right thing and to take into account the risks for the data subject, and those of the company, when collecting or processing personal data.

Once again, I insist on the responsibility of any employee in ensuring compliance. The Compliance Department, cannot, on its own, ensure compliance across the organisation. The role of the compliance department is more a role of facilitator, as it provides a framework, guidance and training in order to support the business to achieve compliance.

HOW DO YOU SEE THE ROLE OF THE DATA PRIVACY OFFICER?

The DPO should be able to provide a clear view on the inherent and residual risks with respect to the collection and processing of personal data. He or she should be aware of the controls that are already in place and should support the implementation of additional controls, where required. He or she is also the person that will ensure that the level of awareness among employees is sufficient and that training is delivered to all employees when needed. He or she is supporting, advising and controlling the data privacy framework, ensuring that policies and procedures are followed and that the risks are under control. In other words, he or she is the person that will provide to the Board a view of the data privacy risks and how they are mitigated.

WHAT ARE THE KEY BENEFITS OF THE INTRODUCTION OF THE PRIVACY BY DESIGN?

The privacy by design is mainly a question of efficiency and cost effectiveness. It is indeed more efficient to properly address a potential issue during the implementation phase then to patch it up once the whole process is designed and up and running. It provides the opportunity to choose the most effective way to achieve the pursued goal.

Finally, it is fully in line with the GDPR risk-based approach as it enables to choose the adequate solution based on the related risks.
Lucas, do you believe GDPR will significantly impact your role at BNP Personal Investors?

GDPR has a clear impact on the organisation. Indeed, due to the sensitivity, the technicality and the regulatory risks, the approach is very much transversal. To be successful, the project should not only be led by the IT department, but, for example, the role of the Legal and the Compliance departments are crucial. It will be crucial to reach a consensus with all stakeholders, who may well have different approaches.

Such consensus is important in adopting a common and pragmatic approach. It should also guard against poor quality results. The emergence of this new Regulation forces the organisation to drastically rethink their data management structure. In order to support such a consensus, it is important to have a group strategy that demonstrates no compliancy.

Does new regulation in general, and GDPR in particular, impact the entire organisation? Does it improve the collaboration or speed it up?

Without this Regulation, the change would have been slower and only a few actors who could foresee that data protection could provide them a strategic advantage would have acted quickly. This, I believe, is also one of the reasons why the transition to GDPR compliance will be easier for some companies more than others.

But with new Regulations and the development of technologies, there is a stronger need for organisational wide coordination. This is one of the reasons behind the development of the role of the Chief Data Officer (‘CDO’). With the emergence of robotics, analytics and the use of data across every sector of the bank, there is an involvement of different stakeholders and the CDO is there to coordinate, leverage and help with the prioritisation.

Of course, for the CDO to facilitate the collaboration and coordination, awareness must be improved at all levels of the organisation. It is therefore important to organise awareness training at an early stage.

GDPR is not just about the bank, it is also mainly about the privacy of data subjects, who are the clients of the bank. Hence, there is not only a need to convince the regulator, but there is also a need to convince your clients and employees that you take good care of their personal data, and that their personal data is safe with you.
Again, for us, the change will be limited in this area as our approach is to maintain a long-lasting relationship with our clients. It has never been our intent to neglect the privacy of our client. Security of customer data is important to our organisation and we see GDPR as an opportunity to reinforce this value.

**DO YOU BELIEVE IT IS STILL POSSIBLE TO USE PERSONAL DATA FROM A MARKETING POINT OF VIEW WITH THE INTRODUCTION OF GDPR?**

We see the emergence of two divergent schools of thought. On the one hand, some actors say that is not possible to use personal data for marketing purposes. On the other hand, there are other actors who believe that if large technology companies continue to use data to push back the boundaries and find new approaches to marketing then why should the financial sector not do so as well. It is my belief that the truth lies somewhere in the middle. Each company should find a reasonable way to use personal data, a way that is aligned with the promises made to the client. So any use of personal information should be legal, transparent and should be expected by the client.

Hence, we will continue to process personal data in compliance with GDPR and we will only do so when it is also in line with our values and with the expectations of the client.

Again, I would like to emphasise the importance of having every stakeholder on board in order to define what we would like to do, if we are authorised to do it and how we intend to use the data. Therefore, a general knowledge of the issues is important, but some deeper dives are also needed.

**DO YOU BELIEVE THAT YOU CAN PRESENT GDPR AS AN OPPORTUNITY, IN ORDER TO INCREASE THE CHANCES OF BUY-IN BY ALL STAKEHOLDERS?**

It is not always easy to demonstrate that a new Regulation can be an opportunity. Nevertheless, it is always important to see the business case for change and seize any change opportunity: to move from a passive compliance point of view to a more proactive implementation that delivers new opportunities.

Moreover, to turn this potential threat into an opportunity you need to get the buy-in from the top management and of the business lines. The regulatory requirements are then embedded by the business lines, rather than just the Compliance function, which mainly focuses on risk mitigation. Likewise, it also makes it possible to leverage the investment in regulatory compliance for business development. Of course, this is an ideal approach, which is not always easy to implement but it should be considered as a target to reach.

**WHAT WOULD BE THE IDEAL ORGANISATIONAL STRUCTURE FOR THE GDPR AND WHERE WOULD YOU PLACE THE DPO?**

There are different approaches for the organisation structure and it will of course be influenced by the regulatory requirements. However, it will also be strongly influenced by the corporate culture and by the people in place. Some organisations seem to be better designed than others.

However, if I had to emphasize one point, it would be that regardless of the organisational structure, it is important to break the silos and to have a
collaborative approach, such as a matrix structure for example. We need to foster a multidisciplinary approach.

In their role, the DPO will also need to adopt a neutral and independent stance. The DPO may not be both judge and jury, and hence we believe that the DPO should be placed in the second line of defence and should remain independent from the business units that he or she is advising and controlling.

Indeed, it will be difficult for the DPO to exercise his or her function if he or she is subject to conflict of interests. How will he or she be able to suggest corrective action if he or she was the one validating the IT infrastructure or security measures in the first place?

**IS THE NEW REGULATION A BRAKE OR AN ENABLER FOR THE IMPLEMENTATION OF NEW TECHNOLOGIES?**

The Regulation in itself does not support the implementation of new technologies: it is our priority to better understand and serve the client. That is the driver for innovation and the introduction of new technologies.

Nevertheless, we need also to recognise that certain technologies are useful for regulatory purposes and are therefore implemented as a consequence of regulatory changes. As an example, I would pinpoint the strong leverage for transaction and fraud analysis. The new technologies enable us to detect patterns or help determine if an alert is a false positive or not.

**FINALLY, COULD YOU EXPLAIN TO US WHAT IS, FOR YOU, THE ADDED VALUE OF THE CONCEPT OF PRIVACY BY DESIGN?**

It is important to remember that GDPR is not designed for banks but it is meant to protect Data Privacy across all sectors of the economy.

The design is probably one of the most important features.

If we take the example of a house. It is more efficient, and indeed easier, to implement functionalities at the beginning. In a house, it is always easier to properly insulate the structure at the build stage as opposed to trying and adopt a corrective measure at a later stage.. The result will be far superior and for a lower cost. From a security and privacy point of view, taking all constraints into consideration from the beginning will also help to increase the efficiency and limit the implementation cost.

Moreover from the client perspective, I believe it is important to know that your privacy will be respected, that you can give your consent and retrieve it. Indeed the client should remain our main focus and we should always take good care of them and keep the promises made.
The purpose of the EU General Data Protection Regulation ('GDPR') is the harmonisation of data protection Regulations across the EU. The Regulation will bring common standards across the EU and make it easier for non EU companies to comply. The goal is to give citizens control over their personal data and to simplify the regulatory environment. Indeed, the Regulation aims to add more clarity to the data processing laws and leave less room for errors. In addition, since the Data Protection Directive was passed in 1995, significant technology changes meant the Directive was lagging behind technological advances and the corresponding creative new uses of personal data.

The GDPR will enter into force on 25 May 2018. With less than one year to go until this compliance deadline, companies from all sectors must keep up with implementation efforts or start as soon as possible in order to be ready on time.

In the recent months, Avantage Reply collected feedback from various financial institutions in relation to the implementation of the Regulation. We found that most companies have made good progress to their planning and work programme. The majority of clients that were contacted have completed a gap analysis stage, defined requirements and are starting to identify solutions to ensure compliance. To be on track for compliance by May 2018, ideally, banks should now be at the implementation stage.

**Figure 1: Path to compliance**
CORE ELEMENTS OF THE REGULATION

The Regulation poses a new three-fold challenge to the financial sector: broader scope, more volume and higher level of complexity. The GDPR retains some key principles introduced by the Data Protection Directive (95/46/EC) and adds a number of new regulatory elements.

In Figures 2 and 3, we highlight the changes introduced by the Regulation and the main points addressed by those changes.

GDPR PRINCIPLES

EU DATA PROTECTION DIRECTIVE (95/46/EC)

6 PRINCIPLES

Lawfulness, fairness and transparency
Purpose limitation
Data minimisation
Accuracy
Storage limitation
Integrity and confidentiality

NEW PRINCIPLE

Accountability

7 PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION

(EU 2016/679)

What is the new principles of accountability?

In a nutshell, the accountability principle refers to the obligation of data controllers not only to comply with the regulatory principles, but also to demonstrate this to the supervisory authorities.

With the responsibility to demonstrate compliance falling upon data controllers, compliance departments will have to re-think their compliance systems based on concepts such as privacy-by-design or privacy-by-default. They will also have to actively engage with the regulators on a series issues. Not the least of these will be the notifications of data breaches.

This new principle is an opportunity for compliance departments to freshly consider the adequacy of current frameworks.

Figure 2: GDPR principles
Two points in particular should focus the attention of compliance departments: the new accountability principle and the shift to a risk-based approach.

Firstly, as per the new accountability principle, the “burden of proof” now falls on regulated entities. Those must take on the responsibility to demonstrate compliance to the regulators.

Secondly, the GDPR introduces a new, “risk-based”, approach to data privacy. The regulation, in its introduction, now frames data collecting and data processing as a “risk to the protection of natural persons”. The new provision, for example, requires that impact assessments are conducted for “high risk” processing. For compliance departments, this means introducing risk assessments of various data processing and linking this with presumably existing classification of data sensitivity.

This new risk-based approach is accompanied by other significant enhancements such as the extension of the definition of territorial reach, the management of “sensitive data” and consent, to list just a few examples.
### GDPR PROVISIONS

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Expanded territorial and conditional scope</td>
</tr>
<tr>
<td>Definitions</td>
<td>Personal data and consent have expanded definitions</td>
</tr>
<tr>
<td>Consent</td>
<td>Further details on validity of consent and children's consent</td>
</tr>
<tr>
<td>Special categories of data</td>
<td>Two new categories: biometric and genetic data</td>
</tr>
<tr>
<td>Rights</td>
<td>Rights listed have been further elaborated, expanded or strengthened.</td>
</tr>
<tr>
<td></td>
<td>Important conditions for each right are listed</td>
</tr>
<tr>
<td>Code of conduct</td>
<td>Modified but remains voluntary and self-relating</td>
</tr>
<tr>
<td>Supervisory authority</td>
<td>Further details on the authority, as well as provisions</td>
</tr>
<tr>
<td>Compensation &amp; liability</td>
<td>Compensation and liability become rights.</td>
</tr>
<tr>
<td></td>
<td>Liability on controller and compensation can be claimed from controller, processor</td>
</tr>
<tr>
<td>Effective judicial remedies</td>
<td>Effective judicial remedies become a right</td>
</tr>
<tr>
<td>Right to lodge complaints with supervisory authority</td>
<td>Rights are strengthened</td>
</tr>
<tr>
<td>Data transfer to third countries</td>
<td>New provisions w.r.t. international organisations, clarity on enforceability</td>
</tr>
<tr>
<td>Certification mechanism</td>
<td>New mechanism, remains voluntary</td>
</tr>
<tr>
<td>Records of processing activities</td>
<td>New mandatory &quot;compliance demonstration&quot;</td>
</tr>
<tr>
<td>Obligations of processor</td>
<td>Obligations of processors are specified</td>
</tr>
<tr>
<td>Data protection officer</td>
<td>Mandatory appointment of Data Protection Officer with defined scope of work</td>
</tr>
<tr>
<td>Data protection impact assessment</td>
<td>Privacy impact assessment mandatory for high risk processing</td>
</tr>
<tr>
<td>Data breach</td>
<td>Mandatory reporting to supervisory authority and data subject, under certain conditions</td>
</tr>
<tr>
<td>Data protection by design &amp; defaults</td>
<td>Obligation to implement efficient internal policies, measures</td>
</tr>
<tr>
<td>Rights: right to data portability</td>
<td>Right of data subject to obtain data in machine-readable format and request direct transfer between controllers</td>
</tr>
<tr>
<td>New definitions</td>
<td>18 (out of 16) definitions are newly added</td>
</tr>
<tr>
<td>Administrative fines</td>
<td>High fines defined for non-compliance, up to EUR 20 min or 4% of the total worldwide turnover</td>
</tr>
</tbody>
</table>

### MODIFIED PROVISIONS

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded territorial and conditional scope</td>
<td></td>
</tr>
<tr>
<td>Personal data and consent have expanded definitions</td>
<td></td>
</tr>
<tr>
<td>Further details on validity of consent and children's consent</td>
<td></td>
</tr>
<tr>
<td>Two new categories: biometric and genetic data</td>
<td></td>
</tr>
<tr>
<td>Rights listed have been further elaborated, expanded or strengthened.</td>
<td></td>
</tr>
<tr>
<td>Important conditions for each right are listed</td>
<td></td>
</tr>
<tr>
<td>Modified but remains voluntary and self-relating</td>
<td></td>
</tr>
<tr>
<td>Further details on the authority, as well as provisions</td>
<td></td>
</tr>
<tr>
<td>Compensation and liability become rights. Liability on controller and compensation can be claimed from controller, processor</td>
<td></td>
</tr>
<tr>
<td>Effective judicial remedies become a right</td>
<td></td>
</tr>
<tr>
<td>Rights are strengthened</td>
<td></td>
</tr>
<tr>
<td>New provisions w.r.t. international organisations, clarity on enforceability</td>
<td></td>
</tr>
<tr>
<td>New mechanism, remains voluntary</td>
<td></td>
</tr>
<tr>
<td>New mandatory &quot;compliance demonstration&quot;</td>
<td></td>
</tr>
<tr>
<td>Obligations of processors are specified</td>
<td></td>
</tr>
<tr>
<td>Mandatory appointment of Data Protection Officer with defined scope of work</td>
<td></td>
</tr>
<tr>
<td>Privacy impact assessment mandatory for high risk processing</td>
<td></td>
</tr>
<tr>
<td>Mandatory reporting to supervisory authority and data subject, under certain conditions</td>
<td></td>
</tr>
<tr>
<td>Obligation to implement efficient internal policies, measures</td>
<td></td>
</tr>
<tr>
<td>Right of data subject to obtain data in machine-readable format and request direct transfer between controllers</td>
<td></td>
</tr>
<tr>
<td>18 (out of 16) definitions are newly added</td>
<td></td>
</tr>
<tr>
<td>High fines defined for non-compliance, up to EUR 20 min or 4% of the total worldwide turnover</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3:** What has changed since the EU data protection directive (95/46/EC)
The GDPR requires wide-ranging changes that will impact organisational structures, people, training, policies, processes, systems and technology support. Some industry actors have long been planning for those changes, for others the GDPR may now seem like an insurmountable mountain.

Whether or not one’s company is well ahead on the path to compliance, we would recommend that the GDPR is taken as an opportunity to reconsider data protection frameworks end-to-end, including the links to other business operations such as sales and data management.

Indeed, regulatory moves worldwide have made one thing very clear: the trend is towards more data protection, not less. In a data-intensive financial industry, understanding and managing data as an asset, with the adequate risk management frameworks, is crucial to remain one step ahead of the regulation and the market.

From the many regulatory changes included in GDPR, we have found that four were of particular interest to our clients. We will address the following topics in the remainder of this section.

1. The right to erasure, or the “right to be forgotten”;
2. The right to data portability;
3. Data breach notification and accountability;

The popularly named “right to be forgotten” is an important tool to contribute to the Regulation’s aim to empower “individuals and give them control over their personal data”. In fact the granted rights are extremely wide, including the right to access, the right to rectification, the right to erasure and the right to restrict processing. Adapting companies’ existing data management processes to respect these new rights will be a significant change for many of our clients.

As the Regulation grants individuals certain rights, such as data modification, data controllers may have no choice but to positively respond to requests when they fall within regulatory provisions. Hence, it is probably important to consider such requests not as potentially rare occurrence, but to consider them as an integral part of personal data management. As such, we would expect to see increasing standardisation of data-handling requests by companies. The ability to automate as much of this process as possible will be key in gaining in efficiency and limiting compliance costs.

It is also important to note that the data controller’s responsibilities towards individuals have also been widened. For example, in the event that personal data, which is subject to a successful request to rectify or erase it, was made public by the data controllers, the data controller must notify others processing that same data of the request. Such new obligations, and others, will require increased internal cooperation, between departments, but also cooperation with external parties such as suppliers.

Those new obligations may also lead DPO and their teams to be in more direct contact with customers. Hence, developing efficient and user-friendly interfaces will be key. In addition,
the management of privacy impact the 'personal meta data', meta data will now need to include all information with respect to how the data is managed and can be modified as well as the extent to which its processing is restricted.

As these new rights become better known by the public, one can expect an increasing number of requests for data modification or erasure. Failure to handle such requests in a swift and professional manner may be harmful in several ways: inefficient processes could quickly become costly and errors in handling requests are likely to have legal, and potential financial, implications. Finally, delays in handling procedures or errors could hurt a brand’s image as data protection is a sensitive topic; this is a risk that companies will definitely want to avoid.

**THE RIGHT TO ERASURE, OR “RIGHT TO BE FORGOTTEN”, CHECKLIST**

<table>
<thead>
<tr>
<th>THE RIGHT APPLIES WHEN</th>
<th>...BUT THERE ARE SOME EXCEPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ The data is no longer necessary for the purpose it was originally collected and processed;</td>
<td>☑ To ensure the right of freedom of expression and of information;</td>
</tr>
<tr>
<td>☑ Consent to processing is withdrawn;</td>
<td>☑ To ensure compliance with the Union or Member State law;</td>
</tr>
<tr>
<td>☑ Processing on legitimate interests cannot be proved;</td>
<td>☑ For a public interest task or exercise of official authority;</td>
</tr>
<tr>
<td>☑ The data is unlawfully processed and in breach of the GDPR;</td>
<td>☑ For public health reasons;</td>
</tr>
<tr>
<td>☑ Compliance with the Union or Member State law needs to be ensured.</td>
<td>☑ For archive, research and statistical purposes;</td>
</tr>
<tr>
<td></td>
<td>☑ If required for the establishment, exercise or defence of legal claims.</td>
</tr>
</tbody>
</table>

*Figure 4: The Right to Erasure, or “Right to be forgotten”, checklist*

**Recommendations for ensuring compliance with these rights**

We recommend that companies establish processes to handle data consent and rectification management:

- Design the company's request-handling process from end-to-end, keeping in mind the necessary interactions between individuals, data controller and data management team.
- Assess to what extent processes dealing with customers’ requests on data can be leveraged on one another by bundling, for example, the customer interfaces or the interfaces within the teams.
- Make sure that all client-facing staff can direct customers and others to the appropriate resource.
  - Make sure the user-friendliness of the customer’s interface to introduce data protection requests.

Companies should also assess the capacity of your current technology solutions in:

- Dealing with such requests and how to best integrate technology support and processes.
- Supporting the necessary controls in data processing, such as the restrictions on
processing data for which requests are pending.

- Finally, we recommend that companies evaluate the cost implications with regard to the right of rectification.

2. The right to data portability will require newly designed processes and technology solutions.

Another important new concept in the GDPR is the right to data portability. This right essentially enhances the already existing individual’s right to access by stipulating that individuals also have the right to receive their data in machine readable format and can request that the data be transferred directly from one data controller to another. Under the GDPR’s provisions, data controllers do not have a right to charge a fee for such services. This may lead to numerous such requests having to be processed, as it’s free for the customer while entities subject to the Regulation bear the increased costs of processing and handling data.

The Regulation stipulates that the right to data portability applies to personal data provided by the individual to the data controller. While this is likely to include data such as information stored on a cloud service, there is still uncertainty with respect to other types of data and it leaves companies with the burden to interpret and identify all areas of data handling affected. It is hence important to note that this right may not apply to financial transactions or purchase histories because such data is created by the data controller and processor while service is provided or a good is purchased.

Further guidance from the supervisory authorities on the scope of this right will be crucial to determine its impact on the operations of the financial services industry. If the scope is indeed strictly limited to data provided to the companies by the data subjects, then it is likely that a significant amount of data held by financial services providers does not fall under the category of data concerned by this provision. In case the scope is broadened and includes data such as financial transaction histories, it is likely to have a serious impact on data management for the financial service industry.

In all cases, the responsibility of data portability does not end when a data controller outsources data to a data processor. The guidance issued by the Article 29 Working Party stipulates that when an outsourcing agreement is in place the responsibilities for data portability must be allocated among parties by means of a contract. This implies that the data controller must ensure that their responsibilities and those of data processors are clearly stipulated and agreed upon. While this may shift the burden of compliance to the data processor, financial institutions will still have to manage the process effectively and incur costs with drafting and managing the contractual arrangements.

There are exceptions to the right to request data portability. In short, a request to data portability should not prejudice the rights of others. Exemptions to the right to portability also include situations when exercising such right would adversely affect IPRs or trade secrets. A conflict between the application of this right and other European or Member State’s law may also lead to exemptions.

This loosely defined scope of the right to data portability, and the question of how this will impact the financial services sector, may lead to uncertainty and some confusion with respect to
its implementation. However, certain steps can and must be already taken, not only to ensure compliance, but also to render compliance as cost-effective as possible.

**Recommendations for ensuring compliance with the right to data portability.**

It is important that companies review the type of customer’s data that they keep on record:

- Data should be categorised based on whether they fall strictly under the scope of the right to data portability, as defined by the Regulation. You could have simple categories such as “portable data”, “potentially portable” or “not portable” in meta-data information.
- An assessment of the size and importance of each category of data in order to evaluate the potential cost of process implementation should be carried out.

Reducing uncertainty for the “potentially portable” category of data should be a priority. This can be achieved, for instance, by submitting a request for clarification to the supervisory authorities or consulting with companies’ legal departments and national laws. Waiting for further guidance from the supervisory authorities is always an option but its consequences should be evaluated.

- We also advise that companies establish processes to handle data portability requests:
- Assess to what extent processes for data portability requests and other types of data requests can be leveraged on one another by bundling, for example, the customer interfaces or the interfaces with the data management teams.
- Design processes end-to-end, keeping in mind the need for interaction between the data controller’s team and the data management teams. A certain level of interaction with legal teams may also be necessary, interactions with third-parties is also likely.
- Standardise, and possibly automate, the handling of and responding to data portability requests as much as possible in order to avoid case-by-case handling of requests. This may be especially important if and when requests numbers rise.

Companies should put the customer first by:

- Consulting within their industry to understand what machine-readable formats are likely to dominate the execution of transfers. Offering a readily compatible format option can only increase customer satisfaction.
- Ensuring the user-friendliness of the customer’s interface to introduce data portability requests.
- Ensuring that all of the client-facing staff are aware of the possibility and guidelines for such requests and can be of relevant assistance to customers.

We also advise that companies assess the capacity of their current technology solutions in:

- Dealing with data portability requests.
- Transferring data, or producing data bulks, in machine readable formats.
- Integrating the handling of such requests with the processes designed.

3. The regulation also imposes requirements for data breach notification and increases the accountability of parties involved in data processing.
A data breach is defined as a breach of security that results in the destruction, loss, alteration, unauthorised disclosure or access to personal data. Those breaches earn significant attention in the Regulation, and in the media, as data controllers will have to maintain an internal breach register. In addition, data processors and data controllers will have to comply with a general requirement to notify the supervisory authorities, within 72 hours of a data breach being identified. Under specific circumstances, data controllers must also notify individuals affected by such breaches.

From a practical point of view, these additional requirements are likely to lead companies to further invest in data security and internal controls. As cyber attacks were recently ranked one of the top risks for 2017 by risk professionals, firms will need not only to sustain investment levels but also conceptualise the management of such risk in a holistically fashion. The substantial fines that are potentially imposed under the GDPR are an additional incentive for firms to fully internalise data security as a priority in risk management.

While data breaches can of course result from cyber attacks, the human factor cannot be discounted and recent history shows that significant breaches caused by mishandling are severely judged by regulators. Hence, both preventive and mitigation measures should be far-ranging: from staff training to internal controls to IT systems. The implementation of robust mitigation measures is also critical as there are now regulatory requirements to the remediation of breaches, such as reporting to the regulator. In disclosng data breaches, potentially also to customers affected by a breach, firms are likely to face reputational challenges given the sensitive nature of personal data as well as media attention. Risk function should fully investigate their exposure to risks of breach, closely follow the evolving cyber attacks and hacking threats and build a picture not just of their defence systems but also of the full impact of a significant breach. Exercises such as recovery planning and ICAAP are likely to be the best forums or opportunities to do this, as well as to allow for leveraging on existing risk understanding.

Complying with this requirement may prove costly. However, there are a number of actions can firms can take, both on the prevention and remediation aspects.

**Recommendations for compliance with data breach notification requirements.**

A first step is to understand a company’s exposure to the risks of cyber attacks and hacking and make such assessments an integral part of operational risks management processes and recovery planning.

Reviewing data security protocols and assessing risk at a more granular level and testing the mitigation measures naturally follows. Importantly, companies should also devise an incident response plan, test it and review such procedures regularly. Incidence response plans must address regulatory requirements, but we would also recommend that particular attention is paid to:

- Handling likely customer complaints in case of incident;
- Reputation’s management, including the firm’s capacity to provide reassurance to markets and customers in a swift and professional manner;
- Assignment of responsibilities in a time of crisis.

It is also worth considering data security as a set of defence layers. In that sense, a first defence
is the protection of the integrity of the data system. If a breach occurs, a second layer could ensure technology led solutions render such data unintelligible, thereby mitigating impact on customer’s privacy and the firm’s sensitive information. Such technology solutions are diverse and understanding their potential will be key in managing this threat.

4. The rules about consent are changing the way data controllers and processors are handling personal data, imposing stricter requirements on what justifies the processing of data

The issue of consent is probably one of the most challenging aspects of the Regulation, due to the new conditions companies have to meet in order to justify the processing of data on legal grounds. GDPR sets a high threshold for consent: requests for consent are only valid when requested separately from other terms and conditions, and should be conveyed in a clear and “unambiguous” manner. Consent for separate processing activities must be requested separately. The Regulation grants a new right to individuals: the right to withdraw consent at any given time. Individuals must be notified of this new right at the time of requesting consent.

Data subjects must also be informed of the procedure to follow to withdraw consent. Hence, forced or “omnibus” consent will not be valid any further. In parallel, due to the newly introduced principle of accountability, data controllers will have to be able to demonstrate that consent was given in accordance with regulatory requirement, and not simply through box-ticking.

The principle of valid consent, when coupled with data transfer to third parties, can become particularly tricky. Tools and processes will need to incorporate information on which third parties will rely on consent being given and on which third parties the firm is relying on for valid consent to be given. And again, simply naming the types of third parties will not be enough.

In brief, valid consent will represent a real challenge to companies as consent has to be continuously and actively managed. Valid consent is likely to have far-reaching consequences. The job descriptions of key client-facing staff, for example, could potentially be modified to incorporate additional responsibilities, and the related capability to handle tools, needed to provide customers with necessary information on consent. Indeed, the further usability of data will depend entirely on this first point of contact.

The issue of consent will pose important questions with respect to the handling of consents for the existing stock of data. Consent given for the existing stock of data may have been given several years prior the rules for data processing came into being... Though the Regulation stipulates that consents given prior to the coming into force of the GDPR may still be valid; there is still the possibility that for certain stocks of data, or parts of datasets, the existing consent would be judged insufficient for further processing.

If that is the case, companies will have to mobilise additional internal and external resources to become compliant and develop tools and processes to reach out to customers for obtaining new consent. Depending on the scale of the exercise, and the associate processes, this may prove to be a significant additional cost, and external resources may turn out to be an appropriate solution. It is therefore important to rapidly assess, if not already done, the extent to which consent given for the existing stock of data is in line with the Regulation. If there is a risk of non-compliance, a temporary set of processes could be put in place to rectify the issue.
As companies are making efforts to get their legal agreements up to par with the Regulation and ensure that they have the appropriate systems and processes in place to obtain valid consent for the processing of data, getting systems ready and training people to ensure that data is processed on lawful grounds is paramount to ensure compliance and avoid fines. Companies may also start exploring other legal grounds for processing data, especially given that consent will still be needed for direct marketing and it is highly unlikely to be obtained. Depending on where you rely on consent a different legal basis may turn out to be right solution for Regulation subjects.

**Recommendations for complying with the rules of consent**

We recommend that companies ensure that their organisation, and staff, are clear about the grounds for lawful processing of data, including exceptions such as the rules for children. We recommend that valid consent is considered as an on-going requirement that has to be actively managed over time. Companies must understand how this can be managed within their existing data management structures and processes and, if necessary, allocate additional resources to the task.

It is essential that consent is active, distinguishable, and not contingent and that individuals are informed of their right to withdraw consent at any time.

Separate consents should be obtained for distinct processing operations and consent should not relied upon when there is a clear imbalance between the data subject and the controller (e.g. the controller is a public authority).

**CONCLUSIONS**

The new Data Protection Regulation is a critical piece of regulation; it is a significant step change when compared to the current data protection regime and it introduces significant potential regulatory penalties. The introduction of a new principle, accountability, and the strengthening and broadening of the DPD’s provisions mean that companies must now re-think their data protection compliance programmes from beginning to end. The new regime, with requirements such as the introduction of a Data Protection Officer and the further definition of data controllers and processors, is likely to encourage the emergence of fully comprehensive data protection compliance programmes that cut across all aspects of a financial service.

**CONSENT CHECKLIST**

**CONSENT UNDER GDPR SHOULD BE:**

- Freely given;
- Specific and informed;
- Distinguishable and in clear and plain language;
- Given by affirmative action;
- Verifiable;
- As easy to withdraw as to give.

*Figure 5: Consent checklist*
provider. It will also make data protection a key concern for client-facing staff, bringing data management closer to the front office. The heavy fine regime introduced by the GDPR will also ensure that this new regime is taken seriously by all industry actors.

The introduction of new supervisory authorities, and an attempt at harmonisation through the European Data Protection Board are a welcome change and crossborder businesses can only hope that further harmonisation ensues. It should also be pointed out that many areas of uncertainty remain in the Regulation. The industry will want to ensure proper representation to the supervisory authorities and the European Data Protection Board in order to obtain further clarifications and specifications on those grey areas. For that reason, and to ensure adequate compliance in the early days of this new regime, close cooperation with the authorities will be essential.

The Regulation presents many challenges but having had two years to achieve compliance financial companies that are among market leaders should now have completed the gap analysis, devised a compliance programme and be now in the solution implementation phase.

The General Data Protection Regulation is a welcome piece of the regulatory puzzle. Its comprehensiveness means that the overall regulatory paradigm with respect to data protection is now set and one can expect further regulatory moves in the same direction.

This brings certainty, even if challenges to achieve full compliance remain. As the Regulation continues to have grey areas and clarifications are still to be issued in the second half of 2017, the compliance programmes have to be actively and closely monitored by Regulation subjects.

**GDPR AND TECHNOLOGY**

In many aspects, the GDPR questions current data management practices that are heavily reliant upon underlying technology. Such regulatory overhaul, likely the most stringent data protection Regulation worldwide, comes with both challenges and opportunities for the tech world. In the years leading to the final approval of the GDPR, we have seen several established tech firms devising tailored solutions for data privacy requirements. Likewise, several start-ups have emerged on the market sometimes offering more innovative products.

The current IT landscape in banks is mostly one of fragmentation, often resulting from merging IT systems after acquisitions, and as such, controlling data collection and propagation though systems, as well as securing data throughout, is likely to challenge those systems. The journey to a better, more secure, way of managing personal data will start with data-mapping. Data-mapping must answer the question of how data propagates through a company’s systems. Based on that knowledge, it will be crucial to devise data governance frameworks, backed up by technology solutions. Data governance should address the question of the nature of data collected and processed as well as their levels of sensitivity, the location of data storage and the authorisation management for both access and consent.
Data governance will also have to include the implementation and management of data security tools. Banks are already familiar with some of those tools, such as encryption and segregation, and may have to quickly become familiar with others, such as pseudonymisation. Data loss protection is also key and is likely to receive regulatory scrutiny.

Several organisations have also moved towards the creation of user-friendly ‘data dashboards’ for customers, along the lines of preference centres. Such dashboards allow customers to manage content and consent of the data provided over their whole lifecycle.

Technology solutions to support this data governance exist, including as add-ons from larger ERP or data management software. In addition, technology solutions are increasingly designed as light add-ons that are plugged into the existing data management systems of firms, and instruct, or pull out data from the system based on a defined set of regulatory requirements. Advantages are obvious for anyone familiar with the costly and resource-intensive IT transformations that firms undertake. However, challenges may remain when it comes to smooth interfaces between systems, which is never a given, or a software’s capability to handle regulatory change.

All solutions on the market tend to combine mature technology with new ones. Two key trends, which go beyond data privacy, are process automation and the use of blockchain technology. The adoption of such new technology solutions may however represent challenges of its own and it is likely that the current regulatory environment is not entirely set up for it.

Moving forward, technology changes and adoption by a broader audience may force Regulation to adapt. And if that is the case, blockchain technology will force the industry to re-think data privacy and management and bring along yet another mini revolution.
Let’s put yourself in the shoes of the Data Privacy Officer of a leading global corporation with millions of users, who tomorrow are asking you to enforce their privacy rights, according with article 13 of the GDPR 679/2016 and with the other articles within the Chapter III of the Regulation.

You will be required to provide to your users the right of access, of rectification and of erasure of their data, and provide them, upon request, with the information related to your processing activities.

Other new requirements such as data portability and the right to be forgotten will add yet another layer of complexity to your role. Add to that, new time restrictions establishing a strict deadline of responding within 30 days and you will begin to see the challenges of your role as Data Privacy Officer at the beginning of the new GDPR regulations.

In fact, you know how quickly and widely data of your users flows throughout your corporation via many different channels, spreading across multiple offices and ICT applications for different purposes, such as provisioning, invoicing, logistics, service delivery, customer care management, to name just a few.

Knowing what user data you hold, who uses it, in which ICT application and system is it stored, and what level of support from suppliers is provided is in fact a very difficult challenge.

Standard approaches based on privacy management tools, or worse mere Excel worksheets or Access databases, fall short and do not relieve the daunting task of retrieving and keeping this information updated.

To this purpose, Spike Reply, the Reply company specialising in Cyber Security, Risk Management & Compliance and System Integration, is proposing a different approach to tackle this complexity, through the development of our Privacy Asset Inventory ('PAI') solution.
The Reply Privacy Asset Inventory (see Figure 6) supports your firm in the collection, storage, retrieval and updating the information you need to ensure the privacy rights of your users. It is based on an open source external Configuration Management Databases (‘CMDB’), integrating multiple sources of data and providing the Data Protection Officer (‘DPO’) and Chief Privacy Officer (‘CPO’) with customisable query engine and reporting features.

**HOW DOES IT WORK?**

The first step is to design a data model schema, which fits into a company’s ICT architecture. The data model schema includes two key aspects: users or customers related information and information related to the company’s ICT assets.

Information related to users, or customers, ranges from customers ID, active contracts and services purchased, to the information concerning the categories of personal data that are processed for the legitimate and necessary purposes of delivering the company’s services to them.

Information related to the company’s ICT assets must also be integrated. Such information comprises, among others, the location of data storage, including the assets locations, serial numbers, IP addresses, software versions, asset owners contact details, and so forth. This information, which must always be up to date and capable of being retrieved within 30 days following a request by a customer.

To build the data model, different data sources must be integrated with the Reply PAI. These include; the Customer Relationship Management (‘CRM’), the Registry of processing activity, and the internal and CMDBs managed by the company’s ICT and Network departments as well as those managed by a company’s suppliers and outsourcers. The integration of these systems facilitates the data feeds into the inventory, which then automates the updating of data.

**PUT IT INTO ACTION**

Imagine again, the CPO in a large multinational company. A user has made a request to the DPO’s team: he, or she, is asking to have his, or her, personal data deleted from the company’s records. The challenges for the CPO, and their team, are numerous. As a start, they must understand what personal data has been stored, where it is stored and how to proceed with erasure. All processes can be facilitated with tools such as the Privacy Asset Inventory.

First, the team responsible for meeting such a privacy request should assess the user, or customer, and his or her request by determining the active contracts and services the customer is currently using. In addition there is also an obligations to identify any non-active services the customer may have used historically or to identify possible data which could fall out of scope from the request itself as for example data which is kept for legal and fiscal purposes.

The next step is for an operator to access the PAI, and write a query to retrieve the information to determine which ICT assets are being used to store the data. Once these categories are known, the operator can then use the query function to retrieve information about the ICT assets along with the details of the ICT assets owners. Technical requests for erasure will then have to be forwarded, according to company processes to the owners of those assets.

Upon fulfilling the technical request, owners of the ICT assets should update the status back into the PAI. Depending on that feedback, the users request can be closed or additional action
taken. The CPO, and their team, can then proceed with notifying the user about the result of his or her request.

Customer’s data requests, such as the request for data erasure as described above, are likely to vary from one industry to another, from one case to another. In order to fit the specific needs of each firm, Reply PAI has a built-in customisable query engine. This allows for the setup of predefined queries, based on the most common user requests received by a company. The customisable query engine speeds up repetitive tasks and minimises the probability of human errors.

Such customised queries could also, for example, take into consideration a company’s legal obligation to keep certain personal data despite a user’s request for erasure. This is useful in situations of claim or fraud management, for example.

Audits and events of personal data breaches are also situations where the CPO and their team will be confronted with challenges for which traditional tools may not be of help. During both audit visits as well as the drafting of data breach notifications, companies are faced with some of the following questions:

- Which users were impacted by the data breach incident, that occurred on this specific asset?
- What security measures were in place to protect the impacted asset?
- When was the last patch applied on the assets impacted?
- Who are the owners of the impacted assets?

All of these questions can easily be addressed with the support of the specific tools available through the Reply PAI.

The Reply PAI is also a useful operative building block to help a company’s GDPR readiness.

The PAI is scalable and flexible due to the open source nature of the underlying technical solution. The PAI has the capability to manage a large number of interfaces which easily integrate the data sources, such as other CMDBs and applications. Data updating is automated through batch data feeds among external sources and the central inventory.

Finally, managing access authorisation for personal data is likely to become increasingly important under GDPR. The Reply PAI allows for the integration of companies’ registries of processing activities into the tool’s workflow engine. This allows the distribution and recording of the processing activities to different actors, each with a specific profile and appropriate access rights to personal data.

GDPR is an opportunity to surf the wave of digital transformation and to streamline internal compliance processes, giving companies the opportunity to focus energy and resources on designing and implementing adequate processes to address the challenge of compliance and to ensure the privacy of their customers. While significant upfront investment in GDPR compliance may seem daunting at first, a well thought through programme of investment is likely to pay off in the mid to long term.

The key to success with GDPR is to create a clear strategy and a holistic vision. Any GDPR technical solution should not be seen as a company’s compliance panacea if it does not align to the existing privacy governance framework.

For over 15 years, Spike Reply has supported its clients in effectively achieving their compliance objectives, setting up sustainable processes, leveraging their unique mix of skills and experiences in system integration and managing advisory on security and data protection topics.
EXTRACT DATA RELATED TO SUPPLIER REPLY SPA TO RENEW ITS CONTRACT WITH ALL INFO REQUIRED BY GDPR

DATA PRIVACY OFFICER

EXTRACT ASSETS AND S.O.P. VERSION DATA RELATED TO CUSTOMERS IMPACTED BY THE RECENT BREACH

HEAD OF IA

INTEGRATE A NEW INVENTORY TO PRIVACY CMDB

ICT, 3P, OUTSOURCER

DELETE MY PERSONAL DATA

CUSTOMER

EXTRACT MY PERSONAL DATA

CRM, INTERNAL & EXTERNAL CMDB

INTEGRATED DATA VIEW OF THE PRIVACY ASSET INVENTORY

Figure 6: Reply Asset Privacy Inventory
## CONTACTS

<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avantage Reply (Amsterdam)</td>
<td>The Atrium I Strawinskylaan 3051 1077 ZX Amsterdam Netherlands</td>
<td>+31 (0) 20 301 2123</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Avantage Reply (Brussels)</td>
<td>5, rue du Congrès/Congresstraat 1000 Brussels Belgium</td>
<td>+32 (0) 2 88 00 32 0</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Avantage Reply (London)</td>
<td>38 Grosvenor Gardens London SWIW 0EB United Kingdom</td>
<td>+44 (0) 207 730 6000</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Avantage Reply (Luxembourg)</td>
<td>21-25 Allée Scheffer 2520 Luxembourg Luxembourg</td>
<td>+352 28 68 43 - 1</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Avantage Reply (Milan)</td>
<td>Via Castellanza, 11 20151 Milano Italy</td>
<td>+39 02 535761</td>
<td><a href="mailto:avantage@reply.it">avantage@reply.it</a></td>
</tr>
<tr>
<td>Avantage Reply (Paris)</td>
<td>Rue du Faubourg Sainte Honoré, 3 75008 Paris France</td>
<td>+33 (0) 1 71 24 12 25</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Avantage Reply (Rome)</td>
<td>V.le Regina Margherita, 8 00198 Roma Italy</td>
<td>+39 06 844341</td>
<td><a href="mailto:avantage@reply.it">avantage@reply.it</a></td>
</tr>
<tr>
<td>Avantage Reply (Turin)</td>
<td>Via Cardinale Massaia, 83 10147 Torino Italy</td>
<td>+39 011 29101</td>
<td><a href="mailto:avantage@reply.it">avantage@reply.it</a></td>
</tr>
<tr>
<td>Avantage Reply (Lisbon)</td>
<td>Avenida da Liberdade, 110 1269-046 Lisbon Portugal</td>
<td>+351 21 340 4500</td>
<td><a href="mailto:avantage@reply.eu">avantage@reply.eu</a></td>
</tr>
<tr>
<td>Xuccess Reply (Frankfurt)</td>
<td>Hahnstrasse 68-70 60528 Frankfurt am Main Germany</td>
<td>+49 (0) 69 669 643-25</td>
<td><a href="mailto:xuccess@reply.de">xuccess@reply.de</a></td>
</tr>
<tr>
<td>Xuccess Reply (Hamburg)</td>
<td>Brook 1 20457 Hamburg Germany</td>
<td>+49 (40) 890 0988-0</td>
<td><a href="mailto:xuccess@reply.de">xuccess@reply.de</a></td>
</tr>
<tr>
<td>Xuccess Reply (Munich)</td>
<td>Arnulfstrasse 27 80335 Munchen Germany</td>
<td>+49 (0) 89 - 41142-0</td>
<td><a href="mailto:xuccess@reply.de">xuccess@reply.de</a></td>
</tr>
</tbody>
</table>