Centre for Information Policy Leadership
Hunton Andrews Kurth

31 May 2019

GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges

The run up to 25 May 2018 was for organisations in the EU and many around the globe a race to GDPR compliance. Both large and small organisations, including those with existing and mature data protection programs in place, have invested significant time and resources to make unprecedented organisational and system changes in anticipation of the new data protection regime. With such great investment comes great expectation that organisations will not only achieve compliance and avoid high, GDPR fines and sanctions and potential reputational damage, but that they will garner the positive impacts associated with responsible data management and a more harmonised and consistent EU data protection framework. In this report, the Centre for Information Policy Leadership (CIPL)[1] seeks to outline the positive impacts and benefits organisations have experienced as a result of their GDPR compliance efforts. We also describe the challenges and unfulfilled promises of the GDPR, where organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements.

The findings of this report are based on CIPL's own observations, a survey of CIPL member experiences with the GDPR and formal discussions through different forums, including CIPL's 2019 Annual Executive Retreat.

Positive Impacts of GDPR	
Data Privacy as a Board Level Issue	**Facilitated top-management focus, buy-in and increased resources for compliance** • The GDPR has resulted in greater awareness and tackling of privacy issues at top management and board level. There are many reasons for this, including potential liability and reputational risks, DPO requirements, increased client requests, the changing nature of relationships with data sharing partners and overall public debate and discourse.
Data Privacy as a Business Enabler	**Shifted view of privacy law from compliance obligation to top business issue and business enabler linked to organisations' data strategy and digital transformation** • The GDPR enabled organisations and their senior leadership to position data privacy compliance as a business enabler, unlocking the potential for organisations to benefit from wider responsible data uses and data driven innovation. Data privacy has been linked firmly to business data strategy and goals, and serves as a competitive advantage.

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 75 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

Organisational Accountability	**Improved organisations' ability to build and implement accountable privacy management programs and demonstrate accountability internally to the Board and externally to regulators, customers, data subjects and shareholders, serving as a potential mitigating factor in case of enforcement** • The GDPR's accountability requirement to comply with data protection principles and to be able to demonstrate such compliance has led to an increased uptake of implementing comprehensive privacy management programs, and to organisations revisiting existing programs to ensure they are up to date. Accountability drives more efficiencies at the organisational level and more effective and better protection for individuals and their data. By putting the burden on organisations handling data, both in the private and public sector, accountability also increases the overall trust in the digital information society and age.
Global Privacy Management Standard for Organisations	**Encouraged organisations to create a single privacy management program for their global operations and entities** • The GDPR has led to many organisations addressing data privacy not only for their EU operations, but also globally across all their business lines, products, services and locations (where appropriate, and taking variations in national law into account). By "putting their house in order", organisations are now dealing with a centralised, streamlined and calibrated privacy program. This enables operational efficiencies for organisations and more consistent protection for individuals.
Higher Data Privacy Awareness and Ownership in Organisations	**Improved overall privacy awareness, data management and sharing tailored to company department specificities, informing important business decisions** • The GDPR has resulted in privacy permeating organisational structures, from top level to various departments and business functions, including engineering, R&D, marketing and HR, all the way down to client/consumer facing functions and roles. This positively impacts organisational culture around data protection generally and strengthens the position and visibility of the privacy office within the organisation.
Greater Business Acumen of Privacy Team	**Acted as a business enabler by giving the data privacy team a seat at the table and bringing business and privacy professionals closer together to discuss how relevant compliance issues align with business goals** • In some organisations, the GDPR resulted in higher visibility of data privacy teams and led them to work cross-functionally with a greater variety of organisational departments. In some cases, this gave privacy teams better insight into business imperatives, how those departments work and the projects they are working on, including technical aspects. It resulted in data privacy teams strengthening their position as trusted business advisers and providing more practical, pragmatic and strategic advice on compliance and in the translation of GDPR requirements into actionable tasks in line with business goals.

Assignment of Internal Responsibility for Data Privacy Governance	**Provided the organisation with an identified expert/team to oversee the privacy management program, implementation of GDPR requirements and ongoing compliance** • The new requirement to appoint a DPO ensured that certain organisations that traditionally did not have a designated member of staff responsible for data protection would integrate one into their organisational structure. It also inspired organisations that are not legally required to appoint a DPO to assign responsibility for data privacy and engage privacy professionals with relevant expertise to assist with GDPR compliance. Among other tasks, data privacy professionals have been reviewing proposed data operations, assisting with risk assessments, creating staff training programs and working with the CISO and security team on breach preparedness and response.
Good Data Hygiene and Management	**Fostered good data hygiene, governance, management and traceability** • The collective impact of several GDPR requirements meant that organisations had to be particularly thoughtful about the data they process. This includes the way they collect, use, share, secure and maintain data within the organisation and with business partners and providers. The obligation to maintain records of processing required organisations to review the data they hold (including customer and employee data), their existing products, services and business lines and the parties with which they share data. In line with the privacy by design principle, organisations also had to review and reassess the relevance and business need for data, in order to ensure data quality, accuracy and retention of only necessary data. Better data management meant not only knowing where and how data is used but maintaining documentation and evidence in relevant product and service processes, including data flow mapping.
Systematic Risk Assessments within Organisations	**Lowered data protection liability risk and supported internal business decisions** • The risk-based approach of the GDPR, including DPIAs, privacy by design requirements and the legitimate interest balancing test have fostered a consistent discipline of assessing risk within organisations – both risks to individuals and risks to organisations. This ensures appropriate risk-based prioritisation of mitigations and controls and a more effective data management program based on actual risk.
Transparency Requirements Generating Trust	**Promoted user-centric and innovative transparency, generating trust in organisations' data handling practices and strengthening relationships both within and outside of the organisation** • The GDPR transparency requirements required a deep dive into the data held by organisations to reach an unprecedented level of transparency both internally, for the organisation and externally to individuals, business partners and regulators. Many organisations modified, or in some cases even completely reinvented, how they engage with individuals to provide information in a more user-centric and design focused way. This created operational efficiencies around the use and accessibility of data within organisations, enhanced customer experience as well as generated external trust and engagement.

Advantage in B2B Negotiations and Due Diligence	**Provided a competitive edge in B2B negotiations and improved ability for organisations to identify trustworthy service providers** • GDPR compliance is an asset in the context of negotiations with business partners who are more likely to deal with GDPR compliant companies in any transactions involving data exchange. This is especially apparent in the selection of processors, where management and security of client/customer data is of paramount importance to companies seeking to engage them. It also increases efficiency in the due diligence processes for selecting appropriate service providers and vendors. A survey of over 3000 senior companies' executives reported that GDPR compliant companies have "better speed to market", with shorter lead-time to negotiate agreements and savings on opportunity costs.[2]
Better Processes for the Exercise of Individual Rights	**Improved organisational processes to facilitate exercise of individual rights** • The GDPR requirements surrounding individual rights required organisations to examine their existing processes for individual rights, update them where necessary and create new procedures in some instances (e.g. creation of data access portals creating a single auditable repository of requests or cross-company efforts to enable data portability, such as, the Data Transfer Project – a joint initiative by Google, Facebook, Twitter and Microsoft).
Breach Readiness and Risk Reduction	**Strengthened organisations' resilience to breaches and prepared them to respond more efficiently** • New GDPR security obligations and requirements to notify breaches to DPAs and individuals under different circumstances meant that organisations proactively reviewed and enhanced their existing data security measures and programs. They also updated their breach response plans and notification procedures, while training staff and management via table-top exercises on new security and data breach handling practices. These investments in continued prevention are lowering organisations' risk of experiencing breaches. When a breach does occur, it is less costly and damaging to the organisation, which can respond in a timely fashion, investigate the issues and take steps to minimise the impact and notify the appropriate regulator(s) and individuals.[3]
Breaking Organisational Silos	**GDPR implementation and ongoing compliance are enterprise-wide processes, requiring multifunctional teams and a joined-up approach between different functions and leadership (CDO, CIO, CISO, CMO, DPO,[4] Legal, Engineering, etc.)** • Organisations that run GDPR implementation as an enterprise-wide and change management project have realised the business benefits of breaking organisational silos between different and often competing functions. The GDPR required a holistic and horizontal approach to data privacy compliance and data management, as the solutions, controls and accountability had to be shared across different functions.

[2] See Maximising the Value of your Data Privacy Investments, CISCO 2019 Data Privacy Benchmark Study, January 2019, available at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf.
[3] *Id*.
[4] Refers to Chief Data Officer, Chief Information Officer, Chief Information Security Officer, Chief Marketing Officer and Data Protection Officer, respectively.

Unfulfilled Promises and Challenges of GDPR	
Lack of Harmonisation Across the EU	**Despite its legal nature and intention, the GDPR has not solved the fragmented privacy landscape in the EU Member States created under Directive 95/46/EC** • As an EU regulation, the GDPR aimed to harmonise data protection rules across Europe. Having a single set of rules across the EU was a strong incentive for organisations to drive operational efficiencies and to offer uniform services and products across the EU Digital Single Market. The promise of harmonisation would also bring legal certainty for individuals in the EU, who are increasingly mobile and participating in cross-border transactions. While the GDPR does provide for a single set of rules to a degree, it fell short of its harmonisation aim. Firstly, Member States, in national laws implementing the GDPR, have made full use of the margin of manoeuvre provided by the GDPR and this has led to the creation of differing rules (e.g. age of consent, processing of sensitive and biometric data, scientific research, etc.). Secondly, national interpretation, guidance and enforcement by DPAs show that there are diverging views, priorities and approaches among DPAs (e.g. differing national lists of high risk processing requiring a DPIA). The EDPB could also play a more proactive role in driving true consistency in the way DPAs interpret and approach data protection rules, compliance and enforcement, and not just through the formal consistency procedure for cross-border processing.
Other Regulatory Bodies Ruling on Privacy Issues	**Non-data protection regulators have started ruling on topics that are within the remit of DPAs** • The GDPR regulates the processing of personal data and establishes that the authorities responsible for enforcement are the Data Protection Authorities (DPAs) under the supervision of the EDPB. However, some other regulatory bodies (such as competition authorities or consumer bodies) have made decisions regarding privacy and data protection issues, where the DPAs (and in cross-border cases the lead DPAs) should be the competent authorities. The EDPB and the DPAs should play a more proactive role in engaging with other regulators to clarify their areas of competence to avoid conflicting and inconsistent rulings.
One Stop Shop Mechanism Not Respected by DPAs	**The One Stop Shop mechanism has not provided organisations with the benefits of interacting with a single regulatory interlocutor in the EU** • There is still ambiguity over the functioning of the One Stop Shop and, in particular, as to whether organisations are able to benefit from a single regulatory interlocutor in the EU. In particular, local DPAs are not respecting the One Stop Shop mechanism as they are sending orders, requests for information, starting audits or imposing fines directly on establishments present in their territory without first involving the lead DPA appointed by the organisations.

GDPR's Territorial Scope Complexities	**The complexity of the GDPR's rules on territorial scope has created a multitude of issues for organisations operating in the international digital ecosystem** • The GDPR applies extraterritorially to organisations outside the EU that offer goods or services to, or monitor the behaviour of, individuals in the Union, by virtue of Article 3. There is a plethora of open issues leading to legal uncertainty about the GDPR's territorial scope. They include the relationship between Article 3 and Chapter V of the GDPR relating to data transfers; the role of the Article 27 representative; whether certain temporary activities constitute the offering of goods or services or monitoring of behaviour, etc. In addition, the rules on the territorial scope of national laws implementing the GDPR within the EU are not clear and create compliance hurdles for organisations operating in and between different EU Member States.
GDPR Interactions with Sectoral Laws	**The GDPR's promise to create a single and uniform set of rules for data protection across Europe has not been realised, due to inconsistencies in sectoral laws** • Despite the comprehensive, risk-based and technology neutral approach of the GDPR, some sector specific laws regulating data use have been or are being adopted or proposed in Europe (e.g. the Payment Services Directive 2 (PSD2), the Clinical Trial Regulation (CTR), as well as the proposed ePrivacy Regulation (ePR)). It is vital that interaction with the GDPR is fully considered when new requirements for data use are introduced. The danger is that sectoral laws (either due to lack of understanding of the GDPR or inconsistent interpretation of the GDPR by other regulators) may undermine the GDPR as the single and ultimate authority on data protection rules in the EU. At this stage, there are some conflicting requirements and no clear rules as to which standard prevails and which authorities will be responsible for enforcing these laws. Even the guidance from the EDPB and national regulators attempting to clear up some inconsistencies has not resolved the challenges for organisations trying to navigate these complex and inconsistent rules. Such legal complexity especially impacts SMEs and start-ups, which do not have resources or access to top legal advice and experienced DPOs. General confusion for organisations around such laws creates risk reticence in terms of data use and may impact the development of new products and services in the EU.

Regulatory Burdens on DPAs	**Effective oversight and enforcement of DPAs through expanded regulatory powers in the GDPR has been obstructed by the requirement to address all complaints and an overly strict interpretation of data breach notification rules** • Under the GDPR, data protection authorities are obliged to handle every complaint they receive, regardless of the risk level involved. This has led to a significant burden on regulators. They spend much of their time and resources in the role of complaint-handler and police officer rather than prioritising their activities based on risks and harms to individuals and focusing their regulatory resources on constructive engagement with organisations and thought leadership activities. In addition to an avalanche of complaints, there is fear that the DPAs are being overburdened with a large number of breach notifications, even when they do not meet the applicable risk or timing threshold. With a real risk of heavy fines, organisations tend to over report. As of May 2019, over 144,000 queries and complaints were made, and over 89,000 data breaches reported, to EU DPAs.[5]
Not Fully Tech Neutral or Future Proof	**Although intended to be technologically neutral and future-proof, the GDPR is not entirely adaptable to new developments in the digital economy** • The GDPR is a principles-based law designed to be future proof and adaptable to emerging technologies and new uses of data. However, several of its provisions (e.g. restricted grounds for processing sensitive data, compatible use, data minimisation, profiling, automated decision-making) and, importantly, their overly strict interpretation, may lead to tensions with artificial intelligence applications, developing biotechnology and blockchain. Even the controller and processor distinction is not adaptable to all scenarios where the roles are not clear or the distinction is not applicable (e.g. Blockchain public networks). In addition, the GDPR embeds the risk–based approach precisely to allow for consideration of risks and harms to individuals and to calibrate compliance based on these risks and harms. There is a general sense that the risk-based approach is often neglected in the official guidance from DPAs and the EDPB. Yet, it is this very approach that would allow the GDPR to stay future proof and continue to adapt to new technologies, especially where they are bringing real benefits for individuals and society at large (provided risks and harms are not severe or likely, or have been mitigated).

[5] See 1 Year GDPR – Taking Stock, European Data Protection Board, 22 May 2019, available at https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

Too Much Focus on Consent and Narrowing of Other Processing Grounds	**For the GDPR to serve as a modern privacy law, its consent requirements cannot be emphasised as the principal legal ground for processing, nor should the other legal bases be continuously construed narrowly.** • Despite the fact that there are six legal basis contained in the GDPR, none of which are privileged over the other, there is a general feeling among data protection practitioners, lawyers and DPOs that DPAs, lawmakers and policymakers in the EU place strong emphasis on consent as a more important legal basis. Legitimate interest, which in most cases provides even more protection than consent, has received less recognition. In addition, there is a perception that DPAs (either deliberately or inadvertently) keep on narrowing the interpretation of all the other grounds for processing. This approach is unrealistic in our data driven society and economy and not in line with the GDPR either. Such emphasis on consent is further reinforced by some "GDPR myths" that have emerged in the marketplace and among the public (e.g. consent is always required for data processing). This forces organisations to revert to consent, even when that is not appropriate and creates consent fatigue for individuals. The consent requirements in the GDPR and their interpretation by the DPAs are also much more complex and stringent compared to other privacy regimes globally (e.g. no possibility for opt-out consent under any circumstances) and do not function well for many modern day data processing contexts and do not provide effective protection for individuals. Finally, the discussions on the ePrivacy Regulation have contributed to further confusion generally on the role of consent, especially as the ePrivacy Regulation risks becoming the pre-dominant rule of internet data use and "trumping" the GDPR.
Lack of Clarity and Consistency Regarding Risk Assessments	**The DPAs have missed the opportunity to fine-tune the risk-based approach in data protection by promoting a clear and consistent approach to assessing risk** • The risk-based approach is firmly enshrined in the GDPR and has been a welcome innovation of the regulatory regime. The GDPR has internalised risk assessment within organisations and they are performing them more frequently. However, the full promise of the risk-based approach has not been realised. There doesn't appear to be a clear and consistent approach to risk assessment. Also, DPAs don't seem to refer to the risk-based approach in their guidance and interpretation or first GDPR enforcement actions, nor do they seem to factor in the benefits of processing in such processes. Although the Working Party 29 Guidelines on risk have been welcomed, overall regulatory guidance to date has been largely unhelpful and fragmented (e.g. numerous national lists of when a DPIA is required has led to unrealistic and unmanageable expectations for organisations). There is a strong feeling that more dialogue and consensus has to be built between organisations and DPAs on how to identify, assess and classify different risks and harms to individuals stemming from data processing.

Unrealised Potential of Certifications and Codes of Conduct as Tools to Demonstrate Accountability	**The potential of GDPR certifications and codes of conduct to demonstrate accountability has not been realised.** • One year after the GDPR went into effect, the regime surrounding GDPR certifications and codes of conduct – which serve as tools for demonstrating organisational accountability – has still not been effectuated. Also, the expected scope of certifications appears unnecessarily limited and not in line with their full potential under the GDPR. For example, certifications are currently envisioned not to cover entire privacy management programs, thereby losing their potential value as comprehensive accountability mechanisms under the GDPR.
Many GDPR Transfer Mechanisms Not Yet Operational	**The framework to use certifications and codes of conduct as transfer tools has not been developed and little progress has been made to expand or improve existing cross-border data transfer mechanisms** • Despite the potential of GDPR certifications and codes of conduct to serve as data transfer tools, the framework to enable their cross-border functions has yet to be developed and such development appears remote. In addition, the 2010 standard contractual clauses are currently facing legal challenge and alternative clauses are not yet available, should the outcome of the Schrems II case invalidate this mechanism. Indeed, much of the 2010 standard contractual clauses are redundant or are in conflict with Article 28 of the GDPR and thus should be reworked as supplemental clauses for processor-importers regardless of whether the exporter is a controller or processor. This would address the current gap in mechanisms for processor to sub-processor cross-border transfers. The 2004 standard contractual clauses should be updated to include data sharing terms, regardless of the geographic location of the controller-importer. Furthermore, BCR were formally recognised in the GDPR and have the potential to expand to entities engaged in joint economic activity. Yet, no work has taken place to expand the use of BCR as a transfer mechanism between different companies, nor to link this important mechanism to accountability obligations under the GDPR or to certifications.
Unrealised potential of BCR	**The BCR's true nature – being a form of certification – has not been recognised and thus not been leveraged for important global interoperability purposes.** • BCR are, at bottom, a certification of a comprehensive privacy program. However, EU DPAs have not recognised this and, as a result, are not able to fully leverage the BCR for purposes of creating interoperability tools and mechanisms between the BCR and other accountability/compliance/transfer certifications, such as the APEC Cross-Border Privacy Rules (CBPR), that would enable organisations to more efficiently become certified/approved in various global accountability schemes that have significant substantive overlap.

As indicated above, the first year of the GDPR has had many positive impacts on industry and, at the same time, presented many unresolved challenges. The positive impacts will continue for responsible organisations who are doing their utmost to comply with the GDPR. The unresolved challenges, on the other hand, will require addressing. CIPL believes that the role of the EDPB and the EU Commission will be pivotal in addressing some of these challenges. One of the prerequisites to solving these issues is

transparency by the EDPB. While there has been some progression in how the EDPB ensures transparency in comparison to the former Article 29 Working Party, CIPL believes that the EDPB, DPAs and industry would benefit from even more constructive engagement, including enhanced transparency, going forward.

In this regard, the consultation process of the EDPB would benefit from and become more efficient by engaging with industry and gathering evidence earlier, in advance of producing initial drafts of guidance. Such engagement could occur via events such as FabLabs, enabling an initial exchange of views on pragmatic interpretations and thinking around GDPR requirements that take into account all stakeholders' views. Alternatively, the relevant EDPB expert subgroup on a particular topic could initiate a pre-consultation phase where it welcomes input from industry on specific topics before the drafting process commences. This would enable organisations and DPOs – who are best placed to provide insights and to comment on technical and operational issues – to further invest time in the process as they would have an assurance that their views might be more appropriately considered than through the current process. It appears that under the current consultation process, very few changes are ultimately made to initial draft versions of the EDPB's guidelines.

DPAs should also play an important role and work with industry through complex issues to enable the GDPR to remain future proof and adaptable to new technologies. A good example of this is the promotion of innovative regulatory models such as the UK ICO's regulatory sandbox initiative.

Conclusion

We hope that by outlining both the positive impacts and benefits experienced from GDPR compliance and the challenges and areas where the GDPR has not lived up to its objectives, organisations and regulators can work together to ensure the GDPR is even more successful in its second year.

If you have any questions or would like additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.