27 April 2017

GDPR Implementation Challenges:

A Summary of CIPL GDPR Project Participants' Feedback

GDPR Implementation Challenges

A Summary of CIPL GDPR Project Participants' Feedback

In early 2017, CIPL asked the participants of CIPL GDPR Project to identify their most important challenges in the process of implementing the GDPR. This paper contains a summary of the feedback from organisations across the range of industries. It does not necessarily reflect the views of CIPL.

This summary provides useful insights into the complex and often resource-intensive process for organisations of becoming GDPR-ready by 25 May 2018. Note also that the challenges identified in this paper may have evolved since the answers were originally provided and since the recent publication of various GDPR guidance by the WP29, which may have addressed some of the open questions.

The paper is organised in two sections. The first section covers overarching high-level concerns, while the subsequent section covers the practical 'nuts and bolts' of GDPR implementation.

I. Summary

The survey illustrates that there are still numerous challenges for organisations in the implementation of the GDPR, and that urgent guidance and further engagement and discussion is needed between the various stakeholders in order to ensure certainty and a feasible framework for the effective implementation of the GDPR. Emphasis must be placed on the overarching objectives of the Regulation to ensure greater protection of the fundamental right of the individual through a user-centric and risk-based approach where real accountability and transparency are the ultimate goals. These can only be achieved through a flexible interpretation of the GDPR where organisations are recognised for taking implementation action in good faith, and a recognition that the implementation process will be ongoing beyond 25 May 2018.

II. Overarching Challenges

1. Ensuring effective regulation and well-resourced DPAs

- The successful implementation of the GDPR depends on organisations executing change management programmes to implement GDPR compliant privacy programs, and DPAs being ready, adequately resourced and organised to embrace their new responsibilities and a new way of operating.

- This is particularly important in order to realise the GDPR's ambitious cooperation and consistency procedures (including one-stop-shop, lead DPA, and the new EDPB).

- The GDPR will bring changes to DPAs and the way they work, both on a national and a European level. DPAs must be fully resourced, effective, and able to execute a harmonised interpretation and approach to the oversight and enforcement of the GDPR. This is essential for the fundamental right to data protection of individuals, as well as the full functioning of the EU Single Digital Market.

- There is a general concern that DPAs may not receive adequate resources from national governments to be able to discharge their increased duties under the GDPR, and engage effectively with stakeholders and within the EDPB, especially given the diversity in sizes and languages.

- DPAs should be able to hire technologists who understand the technological complexities associated with innovation in the digital age.

2. Ongoing and direct dialog with DPAs and the EDPB

- There is a need for greater clarity regarding the working and governance of the EDPB and its efforts to ensure harmonised implementation of the GDPR across Member States.

- The transition from the WP29 to the EDPB needs to be smooth in order to not negatively impact organisations' implementation measures. Organisations need assurance that the WP29 decisions and opinions regarding GDPR implementation will not be contradicted or invalidated by the EDPB, as organisations rely on such guidance in devising implementation programmes.

- There should not be room for divergent interpretations of GDPR concepts by different DPAs issuing national guidance, and taking different views in specific cases.

- Organisations stressed the increased need for cooperation and constructive engagement between controllers/processors and DPAs under the GDPR, especially in the context of the one-stop-shop and the lead DPA mechanism, the consistency mechanism (Arts. 63-66), and in the application of the administrative fines (Art. 83).

- It is critical to ensure dialog between individual organisations (not just industry associations), individual DPAs, the WP29/EDPB, and the European Commission during the transition period and after 25 May 2018, as the GDPR implementation will necessarily continue beyond that date.

- GDPR implementation should be an ongoing and iterative process. The GDPR includes a number of concepts and schemes that can be developed further based on initial implementation experiences (such as standardised policies and icons, certifications and seals, codes of conduct, and further mechanisms for data transfers).

3. Harmonisation, conflicting laws and conflicting interpretations

Persisting issues relating to conflicting laws and conflicting interpretations challenge the effective implementation of the GDPR:

- GDPR harmonisation is an absolute priority and should be the main objective of the implementation during and immediately following the transition period. Eliminating different national interpretations and approaches to implementation is critical for organisations as they develop products, services and technology, interact with consumers, employ people across the EU, and access and transfer personal data across the Digital Single Market.

- The late adoption of implementing legislation in a number of Member States creates a real hurdle for organisations in planning and prioritising GDPR implementation. Organisations ask for transparency and an overview of the status of implementation in each Member State, along with an EU-wide publication of Member State legislation that intersects with the GDPR.

- There is a need to converge the interpretation by Member States of GDPR concepts that may allow for divergent implementation, such as children's age of consent (Art. 8), processing of

special categories of data (including biometric and genetic data) (Art. 9), the exemption for scientific and historical research purposes and statistical purposes (Art. 89), and employees' data processing (Art. 88). Organisations express considerable concern regarding the potential effect of these specifications on harmonisation.

- Organisations also ask for clarification of the interaction between the GDPR and related instruments, including data portability in financial services, NIS Directive, ISO privacy and security standards.

- The ePrivacy Regulation should be interpreted in accordance with the GDPR, and should, as *lex specialis*, not deviate from the forward-thinking privacy-protective provisions of the GDPR. For example, it is important to align the grounds for processing in both regulations, and, in particular, to allow for legitimate interest processing under the ePrivacy Regulation.

- Similar concerns exist for the interaction between the GDPR and other laws and regulations (both EU and third countries'), especially in domains where the co-existence of different requirements may create a conflict of organisations' legal obligations in industries such as financial services and health and pharmaceuticals. For example, other laws may require a data controller to collect sensitive data in order to run compliance checks, and such requirements should prevail over the GDPR.

- There is growing uncertainty regarding the impact of Brexit. Organisations stress the need to consider the consequences for them and the DPAs when the UK ICO will no longer be part of the EDPB and no longer able to act as a lead DPA for one-stop-shop purposes or BCR approvals. The impact on the DPA cooperation (one stop shop, lead DPA), the consistency mechanism and on data transfers to and from UK needs to be clarified.

4. The timing of the GDPR guidance and the costs for organisations

- Organisations expressed concerns that WP29 guidance will come too late or be insufficiently clear for companies to adopt adequate implementation measures. There may be a risk that despite implementation measures undertaken by organisations in good faith, the DPAs will interpret the legal requirements differently and find the measures inadequate come 25 May 2018.

- Some organisations are not able to wait for guidance, yet without more information about interpretation, they find it difficult to prioritise implementation tasks.

- Organisations may have to review or change their implementation programmes post-implementation, which will require re-engineering of and heavy investment in products, services, IT systems and infrastructure. As companies allocate budgets and resources well in advance, untimely guidance may create a lack of available budget when it is needed, impede strategic planning, and undermine the credibility of privacy programmes within organisations.

- This all may impose a considerable burden and create unintended compliance gaps or costs for organisations that ultimately will lead to a negative outcome for individuals.

- On substance, organisations ask the DPAs to keep focus on the main objective of pragmatic, proportionate and risk-based accountability. Assessment of compliance must focus on the right outcomes, rather than a prescriptive adherence to the letter of the GDPR.

- There are fears that guidance may be open for divergent interpretations, or go beyond the letter of the GDPR.

- At the same time, organisations caution against hasty guidance. Some GDPR concepts require prolonged and multi-stakeholder consideration, such as data portability.

III. Substantive Issues in Need of Clarification and Forward Thinking Interpretation

The lack of clarity of interpretation and scope of several GDPR provisions create considerable challenges for organisations:

1. Risk/High Risk

- The risk-based approach is central to the GDPR, and organisations have asked for urgent guidance on how to identify, assess and determine the level of risks to individuals (especially in respect of high risk).

- As stated in an earlier CIPL white paper[1], guidance on high risk must focus on criteria and characteristics of potential high risk processing rather than provide a closed list.

- The definition of 'high risk' will have a wide ripple effect throughout GDPR compliance, so a consistent approach to all risk assessments is essential, irrespective of the provision under which it is performed (DPIA or breach notification, for example).

- Organisations fear divergent national interpretations by the DPAs of the DPIA requirement, especially regarding high risk, and request that WP29 provides a harmonised approach.[2]

2. Legitimate Interest

- Legitimate interest is often appropriate for processing related to network and cyber security, fraud and money laundering prevention, direct marketing and advertising.

- In many cases, legitimate interest is the appropriate legal ground for processing, yet the approach of many DPAs is unclear. Based on different DPA practices, organisations stressed the importance for DPAs to adopt the same view or interpretation of legitimate interest processing.

- Some organisations have identified challenges in applying legitimate interest given the requirement to inform individuals and individuals' right to object. These requirements may pose real practical challenges, for example in relation to fraud prevention, or information security.

---

[1] "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", CIPL GDPR Interpretation and Implementation Project, 21 December 2016. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_project_risk_white_paper_21_december_2016.pfd ;

[2] See also CIPL's white paper on the role of risk, high risk and DPIAs under the GDPR: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pfd.

3. Consent (Arts. 6(1), 7 and 9)

- Consent remains valid and on par with the other grounds for legal processing. However, the GDPR introduces stricter requirements for consent processing, thereby challenging organisations to find ways to counter consent fatigue (as the cookie consent experiences demonstrates). This is a major consideration as new services and products are developed within the Digital Single Market.

- Organisations ask for a productive dialogue with DPAs on how to make consent workable for individuals and organisations in compliance with the new GDPR requirements, such as that consent should be distinguishable, unbundled, based on clear affirmative action, specific, informed, etc. It is not apparent what would qualify as unambiguous or explicit consent mechanisms designed for different customer experiences.

- A smooth transition to the GDPR is needed. Organisations would face a disproportionate high burden should existing consent obtained under the current law need to be revalidated once the GDPR comes into force.

- Consent should remain valid throughout the lifecycle of personal data, unless it is withdrawn.

- The rights to withdraw consent and to object need to be clarified (Art. 7(3)), as they are not absolute. In many cases processing may continue under legitimate interest as the appropriate ground for processing (e.g. fraud prevention, or (global) cyber security threats). Individuals should not be able to freely object or prevent such processing. Similarly, organisations ask for clarification on the individuals' right to object to processing in relation to contracts, such as employment or credit checks.

- It is not clear whether consent can be implied (for data that does not fall under 'special categories'). If it can, it is unclear whether that would require an affirmative action as envisaged by GDPR other than the continuing use of a service, product or feature.

- There are specific concerns regarding children's consent (Art. 8) as there is currently room for different age thresholds (between 13 and 16 years) in different Member States. There are also concerns about how parental consent is verified and obtained. Consent obtained before 25 May 2018 relating to children younger than the age set by a Member State should remain valid once the GDPR comes into force.

4. Data Portability (Arts. 20 and 23)[3]

- The right to data portability remains unclear, making full implementation nearly impossible.

- The recent WP29 guidance expands the scope as defined in the GDPR, and imposes a disproportionate obligation on companies to offer a new service for free.

- Organisations asked for specific confirmation that the data portability right does not apply in many B2B contexts, or to employees' data.

[3] See also CIPL's Comments to the WP29 guidance on data portability: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on-WP29_data_portability_guidelines_15_februart_2017.pdf.

- Sending controllers cannot be expected to assess the appropriateness of a receiving data controller's processing of ported data.

- Many companies struggle to define what conforms to a "structured, commonly used and machine-readable format."

- The category of "observed data" is new. Many organisations find it is too broad and vague, especially as the WP29 states that "it must be interpreted broadly."[4] This may lead to an unjustified impact on IP rights and trade secrets.

- There is a risk that the data portability right may lead to security risks and may be misused by fraudsters who will try to have data downloaded and ported. Questions remain as to how individual's identities will be established as it may require additional information from individuals (which is especially problematic in relation to pseudonymised or de-identified data).

5. Pseudonymised/de-identified data (Arts. 4(5), 32(1)(a) and 40(2)(d), Recitals 26, 28, and 29)

- There is a need to confirm that a controller is not obliged to render pseudonymised data identifiable to comply with rights of access, correction, deletion or portability (Arts. 15, 16, 17, and 20). Organisations also asked for clarification that Art. 11 on "processing which does not require identification" does not require the collection of additional personal data,[5] taking into account the principles of privacy by design and default (Art. 25).

- There should be more flexible application of the requirements of breach notification, data transfers, and further processing for compatible purposes to non-identifiable individuals.

6. Data Breach Notification (Arts. 33, 34 and 83 and Recitals 85, 87 and 88)

- Organisations find the timeframes, conditions and the definition of a reportable data security breach to be particularly challenging. Many note that the expectation to notify breaches within 72 hours is unrealistic and that the term 'undue delay' (Art. 33(1)) therefore must be interpreted flexibly.

- Further work needs to be undertaken to understand the conditions for the notification to an individual, notably the notion of a high risk to the rights and freedoms of individuals.

7. Transparency & Information (Arts. 12(1), 12(5), 12(7), 13 and 14 and Recitals 58-62)

- There appears to be a contradiction between the GDPR's demand for "concise, transparent, intelligible and easily accessible information, using clear and plain language" (Art. 12(1)), and the extensive information to be communicated in privacy notices (Arts. 13 and 14). There is a need for a transparency framework that works for different forms of processing, communications and devices.

---

[4] "Guidelines on the right to data portability", Article 29 Data Protection Working Party, Adopted on 12 December 2016 p. 8. https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/wp242_en_40852.pdf.

[5] Additional data portability concerns, as well as more detail, can be found in CIPL's Comments on the WP29's guidelines on the right of data portability: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on-WP29_data_portability_guidelines_15_februart_2017.pdf.

- Organisations question the definition of "logic involved" in relation to automated decisions, particularly in making this concept accessible and understandable to the individual (Art. 13(2)(f)).

8. The Rights of the Individual (other than data portability) (Arts. 15-17, 18, 21 and 22)

- Organisations raised concerns regarding the scope of individual rights, especially as the right to object (Art. 21, especially in relation to Art. 18 as mentioned below), the rights to access, correction and deletion (Arts. 15. 16, and 17), and the right to no automated decision-making (Art. 22) contain new elements.

- It is not clear how controllers and data processors should give effect to the new right of restriction (Art. 18).

9. Data Transfers and Territorial Application (Arts. 45-50)

- Organisations find it difficult to plan for the extraterritorial application of the GDPR, especially the application to non-EU processors and controllers and to non-EU services such as where a controller is in the EU but offers a service intended for the U.S.

- The need to distinguish what data falls under what jurisdiction is considered a burden for many organisations, as well as the need to reconcile divergent approaches between EU and non-EU jurisdictions for global companies.

- Organisations also experience uncertainty in how the GDPR data transfer provisions will be interpreted by the different DPAs, especially in light of the cases pending before the Court of Justice of the EU.

- Some organisations also express concern that data transfer mechanisms and contractual requirements are at odds with commercial realities; for example, it will be cumbersome to negotiate cloud service terms that may straddle more than one jurisdiction.

- Organisations welcome the EU Commission's communication of January 2017 and the intent to work on extending the existing data transfer mechanisms and adding new ones.

10. Operational Implementation Issues

- Difficulty in prioritising implementation tasks in accordance with a risk-based approach in the face of the uncertainty of how the administrative fines may be levied, or how the different DPAs may enforce the specific GDPR provisions.

- Demonstrating a comprehensive privacy management programme and the level of details required.

- Reviewing existing contracts with third parties. This may pose a disproportionate burden as the number of contracts can run into the hundreds or even thousands.

- Maintaining records of data processing, data mapping and data flows (Art. 24) poses a practical challenge. The level of granularity, continuity, and the specific requirements to documentation continues to vex organisations as they prepare their implementation programs.

- Data protection by design (Art. 25) is another novelty of the GDPR that organisations find difficult to implement. Again, organisations are uncertain of the nature and detail of the required documentation, and the complexity of analysis required by the GDPR.

- There is concern that there currently are no legitimate certifications and codes of practices which organisations can follow that will demonstrate GDPR compliance. Further guidance is needed before certification bodies are established and accredited.

- Some concerns persist regarding the role of the DPO. How can a single person be aware of all processing operations, be ready to demonstrate compliance, and have all the prerequisites required by the GDPR? There is a need for the recognition that this role cannot be interpreted inflexibly or restrictively, but must be adapted to each individual organisation.[6]

- Finally, organisations are concerned about how to inform individuals in a useful manner about retention periods and ask that DPAs recognise the complexities when assessing individual cases.

[6] See also CIPL's white paper on the role of the GDPR DPO and CIPL comments on the WP29's DPO guidelines: https://www.informationpolicycentre.com/uploads/5/7/1/0/571042817/final_cipl_gdpr_dpo_paper_17_november_2016.pfd. https://www.informationandpolicycentre.com/uploads/5/7/1/0/57104281/cipls_commnets_on_wp29_dpo_guidance_24_january_2017.pfd.