Implementing and Interpreting the GDPR: Challenges and Opportunities

"Towards a Successful and Consistent Implementation of the GDPR"

Centre for Information Policy Leadership Workshop Report

Amsterdam, Netherlands
16 March 2016

Dr Asma Vranaki
Fellow

Markus Heyder
Vice President and Senior Policy Counselor

Bojana Bellamy
President

With assistance from the steering committee and members of the CIPL GDPR Project

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On 16 March 2016, the Centre for Information Policy Leadership at Hunton & Williams LLP ("CIPL") and the Dutch Ministry of Security and Justice co-hosted a workshop in Amsterdam entitled "Towards a Successful and Consistent Implementation of the GDPR". The workshop kick-started the special CIPL project ("CIPL GDPR Project") on the consistent interpretation and implementation of the EU General Data Protection Regulation ("GDPR").

The main **objective** of the workshop was to initiate an open and constructive dialogue between industry members, regulators, and policymakers on **two topics**, namely, **"Data Privacy Programmatic Management"** and **"Individual Rights"**.

In this report, we discuss the **eleven key themes** explored during the workshop:

- Ongoing, high-level, and open **engagemen**t between industry, regulators and policy-makers is essential to ensure the consistent implementation and interpretation of the GDPR;

- The Article 29 Working Party and the European Commission will hold several meetings over the next two years which will provide suitable forums for **stakeholder involvement**;

- The **successful GDPR implementation and interpretation** will also depend on various considerations, such as taking into account the aims of the European strategy on the Digital Single Market, devising "future-proof" and technologically neutral guidance, ensuring a harmonised European approach (as far as possible), and considering overlapping European laws (e.g. competition law);

- The centrality of **"accountability"** in the GDPR and importance of incentivising companies to adopt and develop accountability tools;

- How **"smart" data protection regulation** may enable European data protection authorities to discharge their GDPR roles more effectively;

- The importance of clarifying various functional and organisational aspects of the **data protection officer** role;

- The need to develop harmonised understandings of **"risk" and "high risk"**, and agree on **risk assessment approaches and methodologies** that consider not only the risk but also the **benefits** of data processing;

- **Codes of conduct, certifications, seals and binding corporate rules** can be effective compliance and accountability tools if , for example, we incentivise their development and ensure that they work at the "programmatic" rather than product level;

- Implementing and interpreting the rights to **data portability, erasure and object** raise various problems, such as the interactions between data portability and other legal areas (e.g. competition law), which need to be resolved;

- The GDPR **transparency** provisions should be implemented and interpreted in order to minimise any tension which exist between these provisions and the GDPR provisions on detailed notice. Relatedly, we need to carefully consider whether icons are suitable transparency tools; and

- The GDPR will raise specific challenges for **start-ups and small and medium-sized enterprises** which need to be addressed head-on, for example, by involving these organisations in the stakeholder engagement process.

1. INTRODUCTION

1.1 On 16 March 2016, CIPL and the Dutch Ministry of Security and Justice co-hosted a workshop in Amsterdam entitled "Towards a Successful and Consistent Implementation of the GDPR". The workshop kick-started the CIPL GDPR Project.[1]

CIPL GDPR Project

1.2 The **CPIL GDPR Project** aims to establish a forum for an expert dialogue amongst industry representatives, the European data protection authorities ("EU DPAs"), the European Data Protection Supervisor, the EU Commission ("Commission"), the representatives of Member States and academic experts on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and reports. The objectives of the CIPL GDPR Project are set out in **Appendix 1**.

1.3 As set out in **Appendix 2**, the CIPL GDPR Project focusses on **five** topics, namely, (a) data privacy programmatic management, (b) core principles and concepts, (c) individual rights, (d) international data transfers, and (e) the relationships of and with EU DPAs, enforcement and sanctions.

CIPL GDPR Project: Amsterdam Workshop

1.4 The Amsterdam workshop brought together over 100 participants (see **Appendix 5**) from several EU DPAs, the European Data Protection Supervisor, the Commission, government ministries, EU and U.S. businesses, academia and other organisations. The workshop agenda can be found at **Appendix 4**.

1.5 The main objective of the workshop was to initiate an open and constructive dialogue between these stakeholders on two topics, namely, **"Data Privacy Programmatic Management"** and **"Individual Rights"** which were divided into a number of sub-topics (see **Appendices 2 and 4**). We will explore the remaining topics of the CIPL GDPR Project in future workshops, webinars and written outputs (e.g. white papers and reports) (see **Appendices 2 and 3**).

1.6 Relatedly, another objective of the workshop was to track the **four priority areas** of the Article 29 Working Party ("WP29") for 2016.

1.7 In this report, we explore the main takeaway points from **eleven themes** which were explored during the workshop, namely:

1.7.1 Stakeholder engagement;

[1] The proposed Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In this report, we refer to the text of the GDPR which was published on 8 April 2016 following the European Council's adoption of its position at the first reading of the Regulation. The text can be accessed at <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>. On 14 April 2016, the European Parliament approved the GDPR.

1.7.2 Considerations which may impact on the consistent implementation and interpretation of the GDPR;

1.7.3 The priorities of the WP29, the EU DPAs, and the Commission;

1.7.4 Accountability and the GDPR;

1.7.5 "Smart" data protection regulation and the EU DPAs;

1.7.6 The roles of the data protection officers ("DPOs");

1.7.7 The implementation, interpretation and implications of a "risk-based" approach to data protection;

1.7.8 Codes of conduct, certifications, seals and binding corporate rules ("BCRs"); and

1.7.9 Data portability, right to erasure, and the right to object;

1.7.10 Transparency; and

1.7.11 Start-ups and Small and Medium-sized Enterprises ("SMEs").

2. STAKEHOLDER ENGAGEMENT

2.1 The clarion call for a **new culture** of **ongoing, proactive and high-level engagement** amongst industry, privacy professionals, the Commission, the WP29 and the EU DPAs, in order to ensure a truly consistent approach to the GDPR across Europe, resounded very clearly during the workshop.

2.2 The WP29 and the Commission have both issued **open and unqualified engagement invitations** to all stakeholders to provide their input generally on the interpretation and implementation of the GDPR and specifically on:

2.2.1 The priority tasks of the WP29 and the Commission (see **Section 4** below); and

2.2.2 Any other relevant issues (e.g. the age of consent for children).

2.3 To this end, regulators and policy-makers will organise various **engagement meetings** during the two year implementation period of the GDPR. So far, as listed in **Table 1** below, two GDPR stakeholder meetings have been scheduled:

Date	Host	Meeting	Location
September 2016 (Date TBC)	WP29	"FabLab"	Brussels
September 2016 (Date TBC)	Commission	GDPR meeting	TBC

Table 1: Upcoming GDPR Stakeholder Meetings

2.4 During these engagement meetings, **productive dialogue** is key. Given the short implementation time frame for the GDPR and the limited resources of some EU DPAs, stakeholders should not only raise their concerns and issues to the regulators during these meetings but also propose **concrete and workable solutions**.

3. GDPR IMPLEMENTATION AND INTERPRETATION

3.1 All stakeholders agreed that the successful implementation and interpretation of the GDPR depends on a complex set of considerations which we explore next.

The European Strategy on the Digital Single Market

3.2 The GDPR should be implemented and interpreted in light of the European strategy on the digital single market ("DSM") which aims to ensure the free movement of goods, persons, services as well as fair access to online goods and services across Europe. Andrus Ansip, the Vice-President for the Digital Single Market, argues that "[d]ata protection is at the heart of the digital single market; it builds a strong basis to help Europe make better use of innovative digital services like big data and cloud computing."[2]

3.3 The **three main pillars of the DSM** are to:

3.3.1 Provide consumers and businesses with **better access** to digital goods and services across Europe;

3.3.2 Create the right conditions and a level playing field to enable **digital networks and services** to flourish; and

3.3.3 Maximise the growth potential of the **European digital economy**.

3.4 The GDPR explicitly recognises the **twin role** of the Regulation in harmonising the protection of the fundamental rights and freedom of individuals in respect to processing activities and ensuring the free flow of personal data across Europe. The GDPR also explicitly recognises that national differences in the level of protection afforded to the rights and freedoms of individuals may prevent the pan-European flow of personal data which in turn may impact on European economic activities. Accordingly, the GDPR introduces important reforms which aim to assist in building a thriving European data economy which is based on strong data protection standards.

3.5 Consequently, there are **clear synergies** between the aims of the DSM and the GDPR. These connections need to be taken into account by regulators, policy-makers, and privacy professionals when interpreting and implementing the GDPR.

Legal Certainty and Flexibility

3.6 The implementation and interpretation of the GDPR must create as much **legal certainty** as possible *whilst* preserving **flexibility** to support innovation and the DSM. Consequently, any

[2] <http://europa.eu/rapid/press-release_IP-15-5176_en.htm>.

future GDPR guidance issued by the EU DPAs and the Commission needs to be "future-proof" and technologically neutral.

3.7 CIPL believes that in order to stay technologically neutral and "future-proof", successful data protection regulation should be based on a **principles-based approach** which:

3.7.1 Sets out data protection principles in broad terms;

3.7.2 Is outcomes-based; and

3.7.3 Avoids prescriptive details.

3.8 A **principle-based approach** allows for future interpretation and implementation through industry-led initiatives (e.g. seals, certifications, BCRs and codes of conduct) and EU DPA-led guidance, interpretation, supervision and enforcement.

Dynamic and Timely Implementation Guidance

3.9 Any guidance on the implementation of the GDPR must be developed **quickly** considering that the two-year implementation period is not very long, especially when taking into account the budget cycles of organisations.

3.10 Such guidance should also be **evolving** rather than set in stone, as the EU DPAs and the industry build further practical experience in implementing the GDPR over the course of the transition period.

Harmonisation and Consistency

3.11 A key obstacle to the consistent implementation, interpretation and enforcement of the GDPR is the **margin of manoeuvre** that is still open to Member States when it comes to implementing specific GDPR provisions. It is critical that the implementation of the GDPR at Member State level should be as harmonised as possible.

3.12 A minimal degree of local divergence is unavoidable due to differences between Member States (e.g. procedural rules etc.). However, it is imperative to keep such variations to a minimum and reach a consensus on common areas, such as the age of consent for children.

Other Relevant Legal and Regulatory Areas

3.13 The implementation of the GDPR cannot occur in a vacuum, but must be done within the context of other areas of EU law and regulation.

3.14 In particular, when implementing the GDPR, we must also consider **other aspects of EU law** which may conflict with the Regulation. For example, we need to consider the relationship between the GPDR and the E-Privacy Directive,[3] a matter which is currently under review by the Commission.

[3] The Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) as amended by Directive 2009/136/EC ("E-Privacy Directive").

Multi-Disciplinary Collaboration

3.15 The implementation of the GDPR will also require input from **multi-disciplinary experts**, such as engineers, scientist, researchers, and others. It is only by involving a broader range of experts that we can start to resolve some of the challenges raised by the GDPR which do not only require legal answers (e.g. the tensions raised by the transparency and detailed notice obligations).

4. PRIORITIES OF THE WP29, THE EU DPAS AND THE COMMISSION

WP29

4.1 As set out in **Table 2** below, the **WP29** has announced its **four priority areas** with corresponding tasks:

WP29 Priority Areas	Tasks
DPO	• Issue guidelines in 2016
Risk and High Risk	• Issue list of "risky processing" operations • Issue templates and methodology for data protection impact assessments ("DPIAs")
Data Portability	• Issue guidelines in 2016
Certification	• Issue position paper in 2016

Table 2: WP29 2016 Priority Areas

4.2 The WP29 noted that it is considering holding **an online consultation process** before issuing final guidance on its four priority areas. Industry participants expressed their preference for a formalised consultation process which will enable them to provide input and comprehensively raise their views and concerns.

EU DPAs Governance

4.3 Additionally, the **EU DPAs** will develop their governance model under the GDPR. This will include addressing issues of funding and resources, working out their relationships with the European Data Protection Board, and reaching consensus on how the concepts of "one stop shop", the "lead authority" and the "consistency procedure" will work in practice.

Commission

4.4 As for the **Commission**, it only has **two immediate GDPR priorities**, namely implementing Article 50 on international co-operation and addressing the relationship between the GDPR and the E-Privacy Directive. The Commission welcomes input from industry about any other GDPR matter

that it should also work on. In general terms, the Commission is keen to ensure that the implementation of the GDPR leads to harmonisation across Europe.

4.5 Relatedly, the Commission is also keen to hear solutions from industry about the implementation of **Articles 13 and 14** which relate to the information to be provided where personal data are collected from the data subject and where personal data have not been obtained from the data subject respectively.

5. ACCOUNTABILITY

5.1 Over the past years, the **concept of "accountability"** has become a cornerstone of effective data protection and a dominant trend in global data privacy law, policy and organisational practices. From the OECD Guidelines, the APEC Privacy Framework, the U.S., Canada, Mexico, Hong Kong and Singapore to the GDPR, the term encapsulates what most regulators now expect of responsible organisations that handle personal data and what many privacy laws have incorporated as a matter of legal compliance.

5.2 As explored in the earlier CIPL's "Accountability-Based Privacy Governance" project, in simple terms, accountable organisations implement **comprehensive privacy and information management programs**, which encompass various elements including policies, practices, and measures, to ensure that they **comply** with law (including "soft" laws, such as standards and codes of conduct) and can **demonstrate** their data protection compliance to the relevant parties (e.g. the EU DPAs, and the individuals).[4]

5.3 Accountability runs through the core of the **GDPR** which introduces, where applicable, new:

5.3.1 **Accountability obligations** (e.g. appointment of statutory DPOs, DPIAs, data breach notification);

5.3.2 Obligations to **demonstrate accountability** to the EU DPAs and the individuals (e.g. maintain evidence of consent, keep records of the assessment made when relying on "legitimate interests" as the legitimising ground for processing, and retain records of processing operations)

5.3.3 **Accountability relationships** (e.g. processor accountability);

5.3.4 Accountability **verification mechanisms** (e.g. audits); and

5.3.5 Mechanisms to **demonstrate accountability** (e.g. seals, codes of conduct, certifications, BCRs).

These diverse accountability obligations, relationships, and mechanisms can often **interact** with one another. For example, seals, codes of conduct, certifications, and BCRs can be deployed as tools to **demonstrate accountability** as well as to enable organisations to meet their **accountability obligations** and **their obligations to demonstrate accountability**.

[4] CIPL, "Accountability-Based Privacy Governance," <https://www.informationpolicycentre.com/accountability-based_privacy_governance/>.

5.4 **Processors** also need to consider how to become more **accountable organisations** in the context of the GDPR because of their increased statutory obligations, and the scope for joint liability under the Regulation. The GDPR will provide a good opportunity for both controllers and processors to clarify their respective roles, responsibilities and accountability obligations. Such elucidation is likely to have a positive impact on the speed of adoption of new technologies, such as cloud computing and the Internet of Things, in Europe. Additionally, some processors may want to proactively show that they are accountable organisations and use this as a competitive advantage in the B2B context.

5.5 Industry should not operate under the misapprehension that accountability is a substitute for compliance. Instead, accountability enables organisations to **achieve and demonstrate** compliance. However, companies may also often go above and beyond strict compliance with the law as they introduce and implement company-wide policies, measures, and procedures which may be based on a higher or more detailed standard.

5.6 Given the breadth of existing **global guidance on accountability** (e.g. from WP29, Canada, and Hong Kong)[5], it is questionable whether we need further guidance from the EU DPAs or the WP29 on this concept. However, it is important that the accountability concept is fully and consistently understood by all Member States and EU DPAs.

5.7 We should also focus our attention on introducing adequate measures to **incentivise** organisations to adopt and develop accountability measures or tools, such as seals, certifications, and codes of conduct, as well as similar accountability mechanisms, such as the ISO standards.

6. SMART REGULATION AND THE EU DPAS

6.1 The GDPR will also bring significant changes to the roles and powers of EU DPAs at both national and European level. The GDPR provides the need and opportunity to develop new consensus about the evolving roles of EU DPAs, their effectiveness and their relationships with those they regulate.

6.2 In the modern digital economy and being pressed by **limited resources** and the need to be **selective to be impactful**, the EU DPAs may find that they can more effectively discharge their roles as the chief protectors of the fundamental rights of individuals by adopting a **smart approach** to regulation.

6.3 **"Smart regulation"** has various facets including:

6.3.1 Adopting an **"open culture"** by, for example, transparently improving the compliance of organisations with the applicable data privacy laws primarily through guidance and

[5] See Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability 62/10/EN, WP 173 (July 13, 2010), <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf>; Office of the Information and Privacy Commissioner of Alberta et al, "Getting Accountability Right with a Privacy Management Program," (Apr. 17, 2012) < https://iapp.org/media/pdf/knowledge_center/Canada-Getting_Accountability_Right(Apr2012).pdf>; Office of the Privacy Commissioner for Personal Data of Hong Kong, "Privacy Management Programme: A Best Practice Guide," (Feb., 2014) < https://www.pcpd.org.hk/english/resources_centre/publications/files/PMP_guide_e.pdf>.

support rather than sanctions. In the "smart regulation" era, EU DPAs and organisations collaborate with one another to find mutually acceptable solutions;

6.3.2 Promoting **mutual respect** between the EU DPAs and the companies they regulate by, for example, dialoguing productively to reach baseline compliance at a minimum and ideally implement best practice as far as possible;

6.3.3 Adopting **fair and proportionate responses** to actual or potential areas of non-compliance (e.g. using appropriate interventions and sanctions);

6.3.4 Reserving the strongest enforcement actions for **deliberate, wilful, unscrupulous or grossly negligent conduct**;

6.3.5 Recognising that organisations often have plural and overlapping **compliance motivations**, such as increasing the trust of customers and business partners, preventing brand and reputational damage and complying for financial (e.g. avoid a costly lawsuit further down the line) reasons;

6.3.6 Adopting an **incentive-based approach** to compliance which recognises the complex and diverse compliance motivations of companies. Potential incentives could include defences in data breach litigation, reduction in liability, and reputational payoffs. We also need to learn from other industries that have used incentive-based compliance so that we can minimise, as far as possible, the unintended consequences of such incentives (e.g. reward deception which leads to distrust); and

6.3.7 Adopting an **enlightened approach** to compliance which takes into account the business drivers of companies and promotes innovation and the data-driven economy in line with the objectives of the DSM.

6.4 Whilst developing "smart" data privacy regulation, attention needs to be paid to the strategies which will enable EU DPAs to be efficient and effective. Where applicable, such strategies need to take into account the **limited resources** of some EU DPAs.

7. THE ROLES OF THE DPO

7.1 The GDPR mandates the appointment of a DPO in many cases, and prescribes the tasks and responsibilities of the DPOs. The DPOs are essential components of a **data privacy accountability framework** as they play a crucial role in building and implementing data privacy program.

7.2 Industry and regulators should work together and consider various **functional** and **organisational** aspects of DPOs, namely:

7.2.1 Whether DPOs can be completely independent from the companies which employ them?;

7.2.2 Whether the reporting duties of the DPOs to local management can impede the ability of the DPOs to achieve strong data privacy compliance and establish effective privacy programmes in global companies?;

7.2.3 The potential tensions raised by the conflicting expectations that the DPOs will be "independent" from their organisations and their management (i.e. an "internal cop") whilst at the same time being the data protection & privacy leaders, and the trusted team members within their companies;

7.2.4 The potential changes in employment practices required as a result of the "protected" employment status of the DPOs;

7.2.5 The geographic location of the DPOs vis-à-vis the "main establishment" and the multijurisdictional operations of their organisations;

7.2.6 Whether, and if so how, we should differentiate between mandatory and voluntary DPOs? This is particular important in cases where companies appoint DPOs as a matter of best practice; and

7.2.7 How DPOs can avoid conflicts of interests with the other roles and duties that they may have? This is critical to preserving the significance, purpose, and effectiveness of the DPO role.

7.3 When considering these questions, it is important to build on the practices developed by many organisations which have been appointing DPOs for some time. These organisations have developed best practices in terms of ensuring the effectiveness of the appointed DPOs and the ability of the appointed individual to deliver the role.

8. THE RISK-BASED APPROACH OF THE GDPR: INTERPRETATION AND IMPLICATIONS

8.1 A **risk-based approach** means that organisations that handle personal data must implement protective measures which correspond to the level of risk of their processing operations to individuals. In other words, companies should devote more resources to processing activities that pose more risk to individuals who are their customers.

8.2 Under the **GDPR**, accountable organisations have to build and implement compliance programs based on the **"likelihood and severity" of risks** and **potential harms** to the individuals. Additionally, companies may also have data protection obligations which are based on the notion of risk, such as data security and privacy by design. Finally, specific obligations are triggered only in cases of **"high risk" processing**, such as breach notification to individuals and conducting DPIAs.

8.3 The risk-based approach in the GDPR is **useful** because:

8.3.1 It helps organisations and regulators to **prioritise** and **be effective** by focusing compliance on the areas which are most likely to create risks to individuals;

8.3.2 It promotes the development of "**future proof"** and **technologically neutral** rules;

8.3.3 It fosters a **nuanced** rather than a "one-size-fits-all" approach to data protection regulation:

- Compliance is calibrated based on the **actual and concrete risks to individuals**. This places the rights of individuals at the heart of risk evaluation when their rights are balanced with those of companies (e.g. legitimate interest processing ground and further processing).

- However, this does not mean that the **individuals' rights** (e.g. access, objection, and erasure rights) can be modulated according to risk.

8.4 Despite the merits of a risk-based approach to compliance in the GDPR, there are a number of **challenges** ahead including:

8.4.1 Clearly and consistently defining the **concept of "risk"** in Europe. This might involve developing a matrix of harms and threats. CIPL's previous work on a risk-based approach to data protection[6] may be relevant to this topic; and

8.4.2 Developing harmonised guidance on *how* to conduct **risk assessments** including how to conduct the "balancing test" and assess the "likelihood and severity" of risks to individuals.

8.5 During the workshop, industry participants welcomed that the GDPR embraces a risk-based approach to data protection which recognises that effective data protection regulation involves modulating compliance according to an activity's risk level to individuals.

8.6 The WP29 and the Commission were of the view that organisations are best placed to identify and evaluate the **risk level** of their activities. In many cases, companies have already devised comprehensive processes to identify and manage their risks in cases of non-compliance. Consequently, for such organisations, the task ahead is to incorporate the assessment of risk to individuals within these existing processes.

8.7 Industry participants argued that risk assessments must take into account the **benefits of processing**. Risk assessments should also not result in the **unwitting or unnecessary reduction or mitigation** of the benefits of processing. Many industry participants favoured conducting a risk assessment by using the following approach:

Figure 1: Risk Assessment Process

[6] See CIPL, "A Risk-Based Approach to Privacy," (20 March 2014) < https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centres_Privacy_Risk_Framework_Workshop_I_Initial_Issues_Paper.pdf>.

8.8 Some stakeholders also argued that risk analysis should take into account the **risk (particularly to society) of not doing something**. Other stakeholders argued that risk assessments should consider *actual harms* as opposed to the infringement of a fundamental right *without harm*.

8.9 Generally speaking, all stakeholders agreed that **risk assessments and DPIAs** should:

8.9.1 **Be scalable** and designed to avoid **over-reporting of "high risk" activities**; and

8.9.2 Not be too difficult and be **usable by non-experts** in order to ensure their effectiveness as part of the regulatory toolkit.

8.10 Whilst all workshop participants agreed that further work needs to be undertaken on the concepts of "risk" and "high risk", some organisations were **concerned** about:

8.10.1 The usefulness of **pre-determined lists of "risky processing"**. Industry members urged WP29 to consider providing guidance on the objectives and outcomes of risk assessments rather than categorising certain processing operations as "high risk" in advance; and

8.10.2 **DPIA templates** which they viewed as being impractical.

8.11 If regulators and industry do not join hands together to tackle risk appropriately, we will in all likelihood find ourselves in a position where we will have to revert to a regulatory framework which brings **more legal certainty** and **less flexibility**. This is likely to impede innovation and slow down the growth of the data-driven economy in Europe.

9. CODES OF CONDUCT, CERTIFICATIONS, SEALS, AND BCRS

9.1 The GDPR provides for the approval of codes of conduct as well as the accreditation of certifications, seals and marks to help companies demonstrate their compliance with the law. Such mechanisms also enable the law to stay relevant and "future-proof". In addition, the GDPR explicitly recognises BCRs as adequate mechanisms for data transfers outside Europe.

Codes of Conduct

9.2 Codes of conduct have several **benefits** including:

9.2.1 Establishing **best practice** for compliance for specific processing operations;

9.2.2 Enabling companies to commit to, demonstrate, and be recognised for compliance with recognised standards as well as best practice. This will be a **significant competitive advantage** for both controllers and processors in the B2B and B2C context;

9.2.3 Demonstrating that **non-EU data importers** have implemented "adequate safeguards" for the purposes of complying with the data transfer requirements of Article 46; and

9.2.4 Potentially being an **alternative cross-border data mechanism** *on par* with standard contractual clauses and BCRs.

9.3 Some of the most **challenging** aspects of codes of conduct are:

9.3.1 Improving their **development and approval process**. The efficient development of codes of conduct will rely heavily on fruitful dialogues between industry and the EU DPAs. From the Commission's perspective, codes of conduct should be developed by industry;

9.3.2 Devising **incentives** for developing and using codes of conduct; and

9.3.3 Effectively **monitoring** the compliance of organisations with the codes of conduct.

Certifications, Seals and Marks

9.4 Certifications, seals and marks also have many **advantages** including:

9.4.1 Enabling companies to discharge their **accountability obligations** by, for example, demonstrating to others that they have implemented the appropriate technical and organisational measures required by law;

9.4.2 Acting as **strong competitive differentiators** for both controllers and processors in the B2B and B2C contexts; and

9.4.3 Having the potential, in the case of certifications, of being an alternative mechanism for managing and legitimising **cross-border data flows**.

9.5 The upcoming **challenges** for certifications, seals and marks revolve mostly around:

9.5.1 Developing suitable, transparent, and publicly available **accreditation criteria**. This will require collaborative work between industry and regulators. It should be noted that, when it comes to certification regimes, the Commission was again of the view that industry is best place to develop such regimes; and

9.5.2 Ensuring the **scalability** of certifications, seals and marks by encouraging third-party accredited certifiers rather than relying exclusively on the EU DPAs to issue these mechanisms; and

9.5.3 **Incentivising** companies to use these mechanisms.

9.6 The participants also discussed that **going forward**, it is also important that:

9.6.1 Codes of conduct, certifications, seals, and BCRs operate at a **programmatic** rather than merely product level. In other words, they should be important tools in the accountability arsenal of organisations;

9.6.2 Codes of conduct, certifications, seals, and BCRs are all viewed as different accountability tools and are **interoperabl**e with one another as well as other transfer

mechanisms, such as the APEC Cross Border Privacy Rules System, to fully support intra-group as well inter-company cross-border data flows; and

9.6.3 We consider whether the **BCRs** should be assimilated into the certifications and seals category as BCRs are in essence *de facto* seals or certifications awarded by the EU DPAs to accountable organisations.

10. DATA PORTABILITY, RIGHT TO ERASURE AND RIGHT TO OBJECT

10.1 The GDPR also introduces new rights, such as data portability, and enhances existing rights, such as the right to erasure and the right to object, in order to strengthen the rights of individuals. The ability of organisations to comply and show compliance with these rights will form part of their **accountability** obligations.

Data Portability

10.2 Workshop participants discussed at length the new data portability right. All stakeholders agreed that the data portability right aims to empower consumers by enabling them to move their data from one service provider to another. In many ways, the data portability right may redress some of the imbalances between consumers and their data which have emerged over the past years especially in light of the rapid proliferation of data monetisation business models.

10.3 Notwithstanding its intended benefits, **data portability** also raises several **challenges** including:

10.3.1 Its **consistent and effective implementation, interpretation and enforcement** especially when data portability interacts with other legal areas (e.g. intellectual property, competition etc.);

10.3.2 Its potential **impact** on cloud computing, the Internet of Things and data security;

10.3.3 Reducing the **financial burden** faced by companies that have a duty to comply with the data portability obligation. This will prevent competition and innovation from being stifled; and

10.3.4 Its practical problems for **specific sectors**, such as the financial services industry. For example, how do we approach data portability when dealing with joint account holders and complex financial products?

Right to Erasure and Right to Object

10.4 Workshop participants also briefly discussed the new aspects of the **rights to erasure and object** under the GDPR. The discussion revolved around the scope of the right to erasure and the difficulties of implementing both rights in practice. We may explore further the rights to erasure and object in our future GDPR-related work.

11. TRANSPARENCY

11.1 In the GDPR, **transparency** is now an integral part of the data protection principles. Transparency is further reinforced by several other GDPR provisions, such as consent, legitimate interests, information to individuals, right of access, and breach notification. The GDPR also requires communications related to individual rights to be concise, transparent, intelligible, in an easily accessible form and expressed in clear and plain language.

11.2 The GDPR provisions on transparency raise **several challenges and questions** including:

11.2.1 The tension between the GDPR provisions on **transparency** and **detailed notice**. While transparency helps to empower individuals, lengthy and high "legalistic" privacy notices (or equivalent documents) do not deliver real transparency. Such notices are usually drafted mainly to ensure organisations comply with prescriptive provisions of the law. Going forward, we need to determine how to address this tension. One potential way forward could be to involve multi-disciplinary experts, such as psychologists and social scientists, to shed light on the most effective ways in which such information can be communicated to individuals, the right time for such communication, and the right level of information;

11.2.2 How EU DPAs can further incentivise companies to develop and implement **new approaches to transparency**?;

11.2.3 How should transparency requirements be implemented in the context of informing individuals of **further processing** in order to support Big Data?; and

11.2.4 Whether standardised **icons** are effective communication tools? The GDPR empowers the Commission to adopt delegated acts in respect of various matters including icons. The Commission may also carry out appropriate consultation during its preparatory work related to the adoption of specific delegated acts. In exercise of these powers, the Commission will engage an external contractor to undertake a formal study of icons and their roles in enabling organisations to meet their **transparency** and **information obligations** under the GDPR. However, there was substantial concern from industry members that icons may not be effective communication tools.

12. START-UPS AND SMES

12.1 All workshop participants agreed that the consistent and effective implementation, interpretation and enforcement of the GDPR posed significant challenges for both start-ups and SMEs which need to be addressed head-on.

12.2 Effective strategies should be devised to bring start-ups and SMEs to the **stakeholder engagement process**.

12.3 Start-ups and SMEs will also need **specific guidance** on how to apply the **risk-based approach** in their daily processing activities. To that effect, the Commission will provide SMEs with support on implementing the GDPR.

12.4 Some stakeholders argued that **large companies** can also influence how start-ups and SMEs approach data protection compliance. For example, they may carry out in-depth data protection compliance due diligence, insist on and negotiate robust data privacy provisions when contracting with start-ups and SMEs, and educate start-ups and SMEs in accelerators and incubators.

13. NEXT STEPS

13.1 The previously identified priorities by CIPL members align to a large extent with the WP29 priorities, specifically on risk; DPOs; codes of conduct, seals, BCRs and certifications. We will continue following regulatory and legal developments on the important issue of data portability and engage with this topic in the future, if and when necessary.

13.2 As a first step, CIPL will work to develop input on **three WP29 priority areas**, namely, **risk** (including risk, high risk, risk assessments and DPIAs); **DPOs**; and **certifications,** (including seals, codes of conduct and BCRs) as well as evaluate our response to the current public consultation by the Commission on the **E-Privacy Directive**. Our input on certification, seals, codes of conduct and BCRs will also address the concept of accountability generally, whether further accountability guidance is required and using codes, certifications and seals as both accountability and cross-border data transfer mechanisms. We will work on these topics within subgroups composed of CIPL members and other stakeholders.

13.3 Additionally, we will work within subgroups on the following **three CIPL mid-term priority issues**:

13.3.1 Historical and statistical research exemption as well as anonymisation/ pseudonimisation as key levers for the DSM, data-driven innovation and economy;

13.3.2 Core principles and obligations (e.g. consent, children's age of consent, transparency and icons, and legitimate interests); and

13.3.3 Smart regulation (e.g. the roles of EU DPAs, the relationships of EU DPAs with other stakeholders, "one stop shop", main establishment etc.)

13.4 Our input for the work streams set out in Paragraphs 13.2 and 13.3 will involve written submissions, ad-hoc meetings with regulators and policy-makers, participation in formal engagement meetings organised by the WP29 and the Commission, conference calls and webinars, and, of course, our future workshops.

13.5 We have set out our work plan for April to September 2016 in **Appendix 3**.

Appendix 1

OBJECTIVES OF THE CIPL GDPR PROJECT

The CIPL GDPR Project aims to establish a forum for an expert dialogue between industry representatives, EU DPAs, the European Data Protection Supervisor (EDPS), EU Commission, Member States representatives and academic experts through a series of workshops, webinars and white papers with the following specific objectives:

- Informing and advancing **constructive and forward-thinking** interpretations of key GDPR requirements;
- Facilitating **consistency in the interpretation** of the GDPR across the EU;
- Facilitating **consistency in the further implementation** of the GDPR by Member States, EU Commission and EDPB;
- Examining **best practices**, as well as **challenges**, in the implementation of the key GDPR requirements;
- **Sharing industry experiences and views** to benchmark, coordinate and streamline the implementation of new compliance measures; and
- Examining how the new GDPR requirements should be interpreted and implemented to **advance the European Digital Single Market strategy and data-driven innovation**, while protecting the privacy of individuals and respecting the fundamental right to data protection.

Appendix 2

FOCUS TOPICS OF THE CIPL GDPR PROJECT
"5 BUCKETS"

1. **Data Privacy Programmatic Management**
   - Accountability and its elements under the GDPR for controllers and processors
   - Appointment and role of the DPO
   - Assessing risk under the GDPR - privacy impact assessments, privacy by design, breach notification
   - Evidencing and demonstrating accountability externally
   - Privacy seals, certifications, codes of conduct
   - Harmonisation and consistent implementation

2. **Core Principles and Concepts**
   - Legitimacy (consent /age of consent, legitimate interest), decisions based on profiling, transparency, purpose limitation, pseudonymisation

3. **Individual Rights**
   - Data portability, new aspects of data erasure and right to object, transparency

4. **International Data Transfers**
   - Adequacy decisions, BCRs, Model Contracts, the new EU-US Privacy Shield, derogations, seals and certifications, Art. 48, interoperability with non-EU mechanisms

5. **Relationship with DPAs, Enforcement and Sanctions**
   - Smart Regulation
   - Main establishment, One Stop Shop and relationship with EU DPAs
   - Role and powers of the EU DPAs
   - Role and powers of the European Data Protection Board
   - Consistency procedure
   - Sanctions and liability
   - Links with EU strategy for Digital Single Market and Smart Regulation

Appendix 3

CIPL GDPR PROJECT WORK PLAN 2016

PROJECT PRIORITIES AND SUBGROUPS

WP29 and CIPL Initial Priorities

- Risk (including high risk processing and data protection impact assessment (DPIA)
- DPO
- E-Privacy Directive
- Certifications* (including seals, codes of conduct and BCRs and their roles as accountability tools and cross-border transfer mechanisms)

CIPL Midterm Priorities*

- Innovation Drivers (e.g. Historical/statistical research and anonymisation/pseudonymisation)
- Core Principles – Consent (including the age of consent for children), legitimate interest, transparency, notice and icons
- Smart Regulation – The roles of and relationships with EU DPAs, "one-stop-shop" and main establishment

Each topic subgroup will develop and participate in the project activities listed below.

PROJECT ACTIVITIES

Internal	External
• Subgroups and calls • Industry project participants calls - monthly • All project participants calls - every two months • Deep dive webinars	• Workshop reports, papers and written submissions • Ad-hoc engagements with DPAs , Commission and national governments • WP29 FabLab (Brussels) • Workshop II (19 September, Paris) • Workshop III (March 2017, Madrid or Rome, TBC) • European Commission stakeholder day

PROJECT LEADS

- Bojana Bellamy, President, bbellamy@hunton.com
- Markus Heyder, Vice President and Senior Policy Counselor, mheyder@hunton.com
- Richard Thomas, Global Strategy Advisor, richard.thomas@which.net
- Dr. Asma Vranaki, Fellow, avranaki@hunton.com

**Start in Summer*

Appendix 4

CIPL GDPR PROJECT AMSTERDAM WORKSHOP PROGRAM

TOWARDS A SUCCESSFUL AND CONSISTENT IMPLEMENTATION OF THE GDPR

Co-hosted by the Dutch Ministry of Security and Justice

Radisson Blu Hotel, Amsterdam
Rusland 17, 1012 CK
Amsterdam, The Netherlands

16 March 2016 | 9:00-18:00

15 March 2016

18:45 **Pre-Workshop Cocktail Reception**

19:30 **Pre-Workshop Dinner**

- Theatrum Anatonicum (cocktail reception)
  Restaurant-Café In de Waag
  Nieuwmarkt 4, 1012 CR Amsterdam

. . . . . .

16 March 2016

8:30 **Registration**

9:00 **Welcome and Introduction**

- Bojana Bellamy, President, Centre for Information Policy Leadership

9:15 **Special Opening Remarks**

- Alfred Roos, Head of Constitutional and Administrative Law Sector, Department of Legislation and Legal Affairs, Dutch Ministry of Security and Justice

9:30 **Project Objectives and Focus Topics**

Steering group members will introduce and lead an open discussion of project goals and focus topics in the following five categories: (1) Data Privacy Programmatic Management; (2) Core Principles and Concepts; (3) Individual Rights; (4) International Data Transfers; and (5) Relationship with DPAs, Enforcement and Sanctions.[7]

[7] *See* **Appendix 2** for a detailed list of topics.

- ❖ Stephen Deadman, Global Deputy Chief Privacy Officer, Facebook, Inc.
- ❖ Caroline Louveaux, Senior Managing Counsel, Privacy and Data Protection, Legal Department, MasterCard Europe
- ❖ William Malcolm, Senior Privacy Counsel, Google
- ❖ Florian Thoma, Senior Director of Global Data Privacy, Accenture
- ❖ Richard Thomas, Global Strategy Advisor, Centre for Information Policy Leadership

10:15 **Break**

10:30 **Keynote Remarks**

- ❖ Isabelle Falque-Pierrotin, Chair, Article 29 Working Party and President of CNIL
- ❖ Karolina Mojzesowicz, Head of Data Protection Reform Sector, European Commission

11:10 **Open discussion on Project Objectives, Focus Topics and Keynotes**

12:30 **LUNCH**

13:40-17:50 **Workshop I Focus Topic and Discussion**

Each workshop will focus on a subset of the above focus topics. Workshop I will focus on issues relating to Data Privacy Programmatic Management and Individual Rights.

13:40 **Data Privacy Programmatic Management and Focus on the Individual**

Each of the subtopics below will be introduced by designated discussion leads followed by an open discussion with all participants.
(30-35 minutes each subtopic)

- **Accountability and its elements under the GDPR for controllers and processors**
  - Jacobo Esquenazi, Global Privacy Strategist, HP Inc.
  - Stefan Krätschmer, Data Privacy Officer, Europe, IBM Deutschland
  - Manuela Siano, Service for EU and International Matters, Garante per la protezione dei dati personali

- **Appointment and role of the DPO**
  - Cecilia Alvarez, European Data Protection Officer Lead, Spain Legal Director, Pfizer
  - Jacob Kohnstamm, Chairman, Dutch Data Protection Authority

- **Assessing risk under the GDPR - privacy impact assessments, privacy by design, breach notification**
  - Joseph Alhadeff, Vice President of Global Public Policy and Chief Privacy Strategist, Oracle
  - Iain Bourne, Group Manager, UK Information Commissioner's Office
  - Emma Butler, Senior Director Privacy and Data Protection, RELX Group

- Oskari Rovamo, Global Privacy Counsel, Nokia

- **Demonstrating accountability externally, BCR, privacy seals, certifications, and codes of conduct**
  - Joëlle Jouret, Conseiller Juridique, Rechtskundig Adviseur, Belgium Privacy Commission
  - Marie-Charlotte Roques-Bonnet, Director of EMEA Privacy Policy, Microsoft
  - Hilary Wandall, Associate Vice President, Compliance and Chief Privacy Officer, Merck & Co., Inc.

15:40 **Break**

16:00 **Data Privacy Programmatic Management and Focus on the Individual *(continued)*** *(30-35 minutes each subtopic)*

- **Harmonisation and consistent implementation**
  - Rafael García Gozalo, Head of the International Department, Agencia Española de Protección de Datos
  - Donna McPartland, Chief Privacy Official, Corporate Counsel, Compliance Director, GMAC
  - Karolina Mojzesowicz, Head of Data Protection Reform Sector, European Commission

- **Data portability, data erasure, right to object**
  - Vivienne Artz, Managing Director, Head of the International IP and O&T Law Group, Citi
  - William Malcolm, Senior Privacy Counsel, Google
  - Wojciech Wiewiórowski, Assistant European Data Protection Supervisor

- **Transparency to individuals**
  - Piotr Drobek, Deputy Director of the Department of Social Education and International Cooperation, Generalny Inspektor Ochrony Danych Osobowych, Poland
  - Ben Hayes, Chief Privacy Officer, Nielsen

17:50 **Closing Remarks**

❖ Bojana Bellamy, President, Centre for Information Policy Leadership

18:00 **End of Workshop**

Appendix 5

CIPL GDPR PROJECT AMSTERDAM WORKSHOP PARTICIPANTS

Accenture
Acxiom Corporation
Adobe
Agencia Española de Protección de Datos, Spain
American Express Company
AvePoint
Autoriteit Persoonsgegevens (Dutch Data Protection Authority)
Bank of America
Belgium Commission for the Protection of Privacy
Bundesministerium des Innern (BMI), Germany
Citi
Commission de Régulation de l'Énergie, France
Commission nationale de l'informatique et des libertés (CNIL), France
Department of the Taoiseach (Prime Minister's Office) Ireland
Ernst & Young LLP
European Commission
European Data Protection Supervisor
Facebook, Inc.
Garante per la protezione dei dati personali, Italy
Generalny Inspektor Ochrony Danych Osobowych (GIODO), Poland
Google
Graduate Management Admission Council
GSM Association
Guardtime
Huawei
Hudson Advisors
Hunton & Williams LLP
IBM
Intel Corporation
Liberty Global
Lloyds Bank
MasterCard
Merck & Co., Inc.
Microsoft Corporation
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Hungary
Nestle S.A.
Nielsen

Nokia Corporation
Novartis International AG
Nymity, Inc.
Oracle Corporation
Pearson
Permanent Mission of the Kingdom of the Netherlands to the EU
Pfizer, Inc.
Queen Mary University of London
RELX Group
Shell International Ltd.
Sodexo, Inc.
Starwood Hotels & Resorts Worldwide, Inc.
Symantec Corporation
Telefónica S.A.
Teleperformance Group
The Procter & Gamble Company
TRUSTe
UK Department for Culture, Media & Sport
UK Information Commissioner's Office
University of Amsterdam
UPS
Verisk Analytics, Inc.
Vrije Universiteit Brussel
Yahoo! Inc.