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, the European data protection authorities ("EU DPAs"), the European Commission ("Commission"), the ministries of the Member States and academia 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, EU DPAs, the European institutions (e.g. the Commission), the ministries of the Member States and other stakeholders (e.g. privacy professionals) is essential to ensure the consistent implementation and interpretation of the GDPR;

- The Article 29 Working Party and the 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 interpretation and implementation guidance, ensuring a harmonised European approach (as far as possible) and considering the areas of overlap between the GDPR and other European laws (e.g. competition law and the E-Privacy Directive);

- **"Accountability"** is a cornerstone of the GDPR and must be coherently understood by all the relevant stakeholders. Regulators should incentivise companies to adopt and develop accountability tools;

- **"Smart" data protection regulation** may enable EU DPAs to discharge their GDPR roles more effectively and tackle the significant changes in their roles and their powers at national and European levels;

- The **data protection officer** is a linchpin of organisational accountability. It is essential to clarify the functional and organisational aspects of the data protection officer role, in order to ensure the effectiveness of the role;

- The understanding of **"risk"** and **"high risk"** must be harmonised, and effective risk assessment methodologies that consider both the risks and the benefits of processing must be developed and agreed, without determining a definitive list of "high risk" processing;

- **Codes of conduct, certifications, seals and binding corporate rules** can be effective compliance and accountability tools. It would be preferable if they worked at the "programmatic" rather than just the product level only. Regulators should also incentivise the adoption and development of such measures;

- Implementing and interpreting the rights to **data portability, erasure and object** raise various problems which need to be resolved. For example, there are potential interactions between the data portability right and other legal areas, such as intellectual property, which need to be tackled effectively;

- The GDPR **transparency** provisions should be implemented and interpreted in order to minimise any potential tension between the GDPR provisions on transparency and detailed notice. Relatedly, the relevant stakeholders should 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 start-ups and small and medium-sized enterprises in the stakeholder engagement process. Also, stakeholders might explore how larger and more experienced companies can help shape how start-ups and small and medium-sized enterprises approach data protection compliance.

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 **CIPL GDPR Project** aims to establish a forum for an expert dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the Commission, the ministries of the 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 focuses 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[2] from several EU DPAs, the European Data Protection Supervisor, the Commission, the ministries of various Member States, EU and US businesses, academia and other organisations.

1.5 As set out in the workshop agenda (see **Appendix 4**), the main objective of the workshop was to initiate an open and constructive dialogue between the stakeholders on two topics, namely, **"Data Privacy Programmatic Management"** and **"Individual Rights"**.[3] The **"Data Privacy Programmatic Management"** topic focussed on accountability and its elements under the GDPR, the role of the data protection officer ("DPO"), the risk-based approach in the GDPR, seals, certifications and codes of conduct as well as harmonisation and consistent implementation. The **"Individual Rights"** topic considered data portability, new aspects of the right to erasure and the right to object as well as transparency.

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] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ L 119/1 < http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN >. The GDPR will apply on 25 May 2018.

[2] See **Appendix 5**.

[3] See **Appendices 2 and 5**.

a. Stakeholder engagement;

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

c. The priorities of the WP29, the EU DPAs and the Commission;

d. Accountability and the GDPR;

e. "Smart" data protection regulation and the EU DPAs;

f. The roles of the DPOs;

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

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

i. Data portability, right to erasure and the right to object;

j. Transparency; and

k. 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** between all stakeholders including industry members, privacy professionals, the ministries of the Member States, 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. If all stakeholders do not work collaboratively to ensure the consistent implementation, interpretation and enforcement of the GDPR, 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 weaken the protection of the fundamental rights of individuals, impede innovation and slow down the growth of the data-driven economy in Europe. The CIPL GDPR Project will play a pivotal role in supporting stakeholder engagement on the implementation, interpretation and enforcement of key GDPR provisions through its diverse activities in this area.[4]

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:

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

[4] See **Appendix 3**.

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

2.3 To this end, regulators and policymakers 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
July 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 Workshop participants agreed that the successful implementation and interpretation of the GDPR depends on a complex set of considerations which we explore next.

Legal Certainty and Flexibility

3.2 The implementation and interpretation of the GDPR must create as much **legal certainty** as possible for the protection of the fundamental rights of individuals *whilst* preserving **flexibility** to support innovation in Europe and the European strategy on the digital single market ("DSM"). Consequently, any future GDPR guidance issued by the EU DPAs and the Commission should, as far as possible, be "future-proof" and technologically neutral as well as ensure flexible and effective context-specific compliance.

3.3 CIPL believes that in order to stay technologically neutral and "future-proof", the implementation and interpretation of the GDPR should use a **principles-based approach** which:

a. Interprets data protection principles in broad and flexible terms;

b. Is outcomes-based; and

c. Avoids prescriptive details.

3.4 A **principle-based approach** to the **implementation and interpretation of the GDPR** allows for future context-specific interpretation and implementation at the company level or through industry-led initiatives (e.g. seals, certifications, BCRs and codes of conduct). It also enables effective guidance, interpretation, supervision and enforcement by EU DPAs.

Harmonisation and Consistency

3.5 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.

3.6 A minimal degree of local divergence is unavoidable due to differences between Member States (e.g. procedural and cultural differences). However, there is room for Member States to develop a consensus on how to locally implement the "open clauses" in the GDPR. In order to ensure that the GDPR achieves its objectives,[5] it is imperative to keep local variations to a minimum and reach a consensus on common areas, such as the age of consent of children and the rules on the processing of the personal data of employees in the employment context.

DSM

3.7 The GDPR should be implemented and interpreted in light of the **DSM** which aims to ensure the free movement of goods, persons and 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."[6]

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

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

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

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

3.9 The primary **objective** of the GDPR is to protect the fundamental rights and freedom of individuals in respect to the processing of their personal data. The GDPR also aims to ensure the free flow of personal data across Europe. National differences in the level of protection afforded to the rights and freedoms of individuals may prevent the transborder flow of personal data which in turn may impact on European economic activities. The GDPR should significantly reduce the differences amongst the regimes of data protection laws of the Member States. The GDPR reforms should also assist in building a thriving European data economy which is based on strong data protection standards.

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

[5] See Paragraph 3.9 below.
[6] <http://europa.eu/rapid/press-release_IP-15-5176_en.htm>.

Dynamic and Timely Implementation Guidance

3.11 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.

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

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, the relevant stakeholders must also consider **other aspects of EU law** which may conflict with the Regulation. For example, the relevant stakeholders need to consider the relationship between the GDPR and the E-Privacy Directive,[7] a matter which is currently under consideration by the Commission. The Commission has recently initiated a public consultation on the review and evaluation of the E-Privacy Directive.[8]

Multi-Disciplinary Collaboration

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

[7] The Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) as amended by Directive 2009/136/EC ("E-Privacy Directive").
[8] <https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive>.

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 "high risk" 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 has only **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 would like input from the stakeholders on the delegated and implementing acts that it should adopt, the solutions related to 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 and any other GDPR matter 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.

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 and the accountability guidelines from Canada, Mexico, Hong Kong and Singapore to the GDPR, the term "accountability" encapsulates what most regulators now expect of responsible organisations that handle personal data and what many data 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 programmes**, 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).[9]

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

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

b. 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);

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

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

e. Mechanisms to **demonstrate accountability** (e.g. seals, codes of conduct, certifications and 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 by organisations as tools to **demonstrate accountability** as well as to meet their **accountability obligations**.

5.4 **Processors** also need to consider how to become more **accountable organisations** in the context of the GDPR because of their increased legal 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. Evidently, this is not the aim of the GDPR but rather an example of one of its potential positive side-effects.

5.5 Additionally, processors may want to proactively show that they are accountable organisations and use this to signal their commitment to protecting the **fundamental rights and freedoms** of individuals as well as a **competitive advantage** in the B2B context.

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

5.6 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.

5.7 Given the breadth of existing **global guidance on accountability** (e.g. from WP29, Canada and Hong Kong)[10], relevant stakeholders need to build on such guidance rather than start afresh. It is also important that all stakeholders fully and consistently understand the accountability concept.

5.8 The regulators should also focus their attention on incentivising 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 levels. 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 CIPL strongly believes that 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 and freedoms of individuals by adopting a **"smart" approach** to regulation.

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

a. Adopting an **"open culture"** by, for example, transparently improving the compliance of organisations with the applicable data privacy laws primarily through guidance and support rather than sanctions. In the "smart regulation" era, EU DPAs and organisations collaborate with one another to find mutually acceptable solutions;

b. 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;

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

[10] 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>.

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

e. 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. to avoid a costly lawsuit further down the line) reasons;

f. 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. Stakeholders also need to learn from other industries that have used incentive-based compliance so that the unintended consequences of such incentives (e.g. reward deception which leads to distrust) can be minimised, as far as possible; and

g. 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.

7. THE ROLES OF THE DPO

7.1 The GDPR mandates the appointment of DPOs 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 a data privacy programme.

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

a. To what extent is the "independence" of the DPO desirable and/or mandated by the GDPR?;

b. The potential tensions raised by the 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;

c. Whether, in the case of global companies, 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?;

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

e. The geographic location of the DPOs vis-à-vis the "main establishment" and the multi-jurisdictional operations of their organisations;

f. 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

g. 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 that can effectively deliver the role for some time.

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

8.1 A **risk-based approach** to data protection means that organisations that handle personal data must implement protective measures which correspond to the level of risk of their processing operations to the fundamental rights and freedoms of 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 programmes based on the **"likelihood and severity" of risks** and **potential harms** to the fundamental rights and freedoms of individuals which may result from personal data processing (e.g. physical, material or non-material damage, such as discrimination, identity theft or fraud, financial loss, loss of confidentiality of personal data protected by professional secrecy and preventing data subjects from exercising control over their personal data). 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:

a. 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;

b. It promotes the development of "**future-proof"** and **technologically neutral** rules; and

c. 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 the fundamental rights and freedom of 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 the risk level of the personal data processing in question.

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

a. Clearly and consistently defining the concepts of **"risk" and "high 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[11] may be relevant to this topic; and

b. 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 the rights and freedoms of 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 the rights and freedoms of 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 start with and take into account the **benefits (or purposes) of processing** to individuals and society. An understanding of the benefits of processing is necessary to implement appropriate risk mitigation measures that do not unwittingly or unnecessarily reduce the benefits of processing activities. Many industry participants favoured conducting a risk assessment by using the following approach:

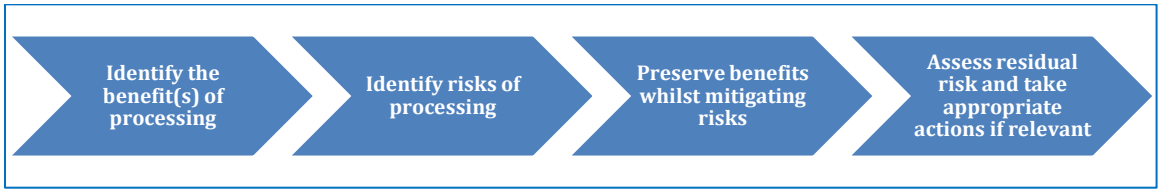

Figure 1: Risk Assessment Process

8.8 Some stakeholders also contended that risk analysis should take into account the **risk (particularly to society) of not doing something**. Other stakeholders were of the view that risk

[11] 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>.

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:

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

b. 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:

a. 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

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

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 as well as meet their accountability obligations under 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:

a. Establishing **best practice** for compliance for specific processing operations;

b. Enabling companies to commit to, demonstrate and be recognised for compliance with recognised standards as well as best practice. Codes of conduct will be **key accountability tools** which can be used by organisations to show to individuals and their regulators that they protect the fundamental rights and freedoms of individuals in accordance with the law. Additionally, codes of conduct can also have significant competitive advantage for both controllers and processors in the B2B and B2C contexts;

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

d. 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:

a. 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;

b. **Incentivising** the development and adoption of the codes of conduct; and

c. 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:

a. 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 in order to protect the fundamental rights and freedoms of individuals;

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

c. 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:

a. 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 best placed to develop such regimes;

b. 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

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

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

a. 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;

b. Codes of conduct, certifications, seals and BCRs are all viewed as different accountability tools and are **interoperable** 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 as inter-company cross-border data flows; and

c. Stakeholders 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 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:

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

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

c. 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

d. 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 to 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 to 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:

a. 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.

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

c. How can transparency be used to inform individuals of **further processing** in the context of innovative technologies, such as Big Data, Internet of Things, machine learning and artificial intelligence?; and

d. 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** to data protection 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, large companies 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; and 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 to evaluate its response to the current public consultation by the Commission on the **E-Privacy Directive**. CIPL`s 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. CIPL will work on these topics within subgroups composed of CIPL members and other stakeholders.

13.3 Additionally, CIPL will work within subgroups on the following **three midterm priority issues**:

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

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

c. 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 CIPL`s input for the work streams set out in Paragraphs 13.2 and 13.3 will involve written submissions, ad hoc meetings with regulators and policymakers, participation in formal engagement meetings organised by the WP29 and the Commission, conference calls and webinars, and, of course, future workshops.

13.5 CIPL's work plan for May to September 2016 is set out 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), the Commission, the 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, the 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 DSM 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; and
   - 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 the EU 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 EDPB;
   - Consistency procedure;
   - Sanctions and liability; and
   - 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 DPIAs);
- DPO;
- E-Privacy Directive; and
- 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; and
- 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 EU DPAs, European Commission and national governments • WP29 FabLab (Brussels) • Workshop II (September, Paris TBC) • Workshop III (January 2017, Brussels 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 2016*

Appendix 4

CIPL GDPR PROJECT AMSTERDAM WORKSHOP PROGRAMME

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.[12]

[12] *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 Álvarez, 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

Joseph Alhadeff	Oracle Corporation
Cecilia Alvarez	Pfizer, Inc.
Vivienne Artz	Citi
Maria Chiara Atzori	Novartis International AG
Carmen Barrett	Pearson
Bojana Bellamy	Centre for Information Policy Leadership
Katinka Bojnár	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), Hungary
Machiel Bolhuis	Liberty Global
Iain Bourne	UK Information Commissioner's Office
Emma Butler	RELX Group
Ilias Chantzos	Symantec Corporation
José Checa	Nestle S.A.
Sinead Connolly	Facebook, Inc.
Cameron Copeland	Bank of America
Stephen Deadman	Facebook, Inc.
Nancy Dean	Verisk Analytics, Inc.
Adelaide Deleplanque	Liberty Global
Ulrika Dellrud	Oracle Corporation
Robert Donohoe	Hudson Advisors
Belinda Doshi	Pearson
Piotr Drobek	Generalny Inspektor Ochrony Danych Osobowych (GIODO), Poland
Francois-Xavier Dussart	Yahoo! Inc.
Nico van Eijk	University of Amsterdam
Patrice Ettinger	Pfizer, Inc.
Daniela Fabian Masoch	Centre for Information Policy Leadership Fellow
Isabelle Falque-Pierrotin	Commission nationale de l'informatique et des libertés (CNIL), France
Anne Flanagan	Queen Mary University of London
Stuart Fowkes	Hudson Advisors
Christine Frye	Bank of America
Joanne Furtsch	TRUSTe
Rafael García Gozalo	Agencia Española de Protección de Datos
Raphaël Gellert	Vrije Universiteit Brussel
Helen Graham	Shell International Ltd.
Joris Groen	Dutch Ministry of Security and Justice
Dominique Hagenauw	Dutch Data Protection Authority

Adrienne Harrington	Department of the Taoiseach (Prime Minister's Office), Ireland
Paul Harris	Sodexo, Inc.
Josh Harris	TRUSTe
Benjamin Hayes	Nielsen
Markus Heyder	Centre for Information Policy Leadership
Hielke Hijmans	University of Amsterdam/Vrije Universiteit Brussel
Shirin Huber	UPS
Peter Hustinx	Former European Data Protection Supervisor
Elena Irimia	Merck & Co., Inc.
Daniel Jin	Centre for Information Policy Leadership
John Jolliffe	Adobe
Jeroen de Jong	Dutch Ministry of Security and Justice
Joëlle Jouret	Belgium Commission for the Protection of Privacy
Irene Kamara	Vrije Universiteit Brussel
Jacob Kohnstamm	Dutch Data Protection Authority
Stefan Krätschmer	IBM Deutschland GmbH
Michael Lamb	RELX Group
Adriana Lopez-Tafall	Merck & Co., Inc.
Caroline Louveaux	MasterCard
Jessie Luo	Huawei
Aylin Lusi	UPS
William Malcolm	Google UK Limited
Riccardo Masucci	Intel Corporation
Donna McPartland	Graduate Management Admission Council
Terry McQuay	Nymity, Inc.
William Min	Starwood Hotels & Resorts Worldwide, Inc.
Karolina Mojzesowicz	European Commission
Rory Munro	UK Department for Culture, Media & Sport
Kirsten Mycroft	Lloyds Bank
Wim Nauwelaerts	Hunton & Williams LLP
Udo Oelen	Dutch Data Protection Authority
Nicola Orlandi	Novartis International AG
Yann Padova	Commission de Régulation de l'Énergie, France
Dragan Pendić	Guardtime
Ross Phillipson	The Procter & Gamble Company
Jan Rinia	Permanent Mission of the Kingdom of the Netherlands to the EU
Alfred Roos	Dutch Ministry of Security and Justice
Marie-Charlotte Roques-Bonnet	Microsoft Corporation
Oskari Rovamo	Nokia Corporation
Steve Satterfield	Facebook, Inc.
Sachiko Scheuing	Acxiom Corporation

Sarah Shaw	Hudson Advisors
Manuela Siano	Garante per la protezione dei dati personali, Italy
Dana Simberkoff	AvePoint
David Smith	Nymity, Inc.
Jennifer Stoddart	Nymity, Inc.
Florian Thoma	Accenture
Richard Thomas	Centre for Information Policy Leadership
Louise Thorpe	American Express Company
Allen Ting	Huawei
Monika Tomczak-Górlikowska	Shell International Ltd.
Wilbert Tomesen	Dutch Data Protection Authority
Sophie Vannier	Commission nationale de l'informatique et des libertés (CNIL), France
Winfried Veil	Bundesministerium des Innern (BMI), Germany
Ryan Vinelli	Starwood Hotels & Resorts Worldwide, Inc.
Cristina Vela	Telefónica S.A.
Anneke Vissers	Ernst & Young LLP
Asma Vranaki	Centre for Socio-Legal Studies, University of Oxford
Hilary Wandall	Merck & Co., Inc.
Wojciech Wiewiorowski	European Data Protection Supervisor
Alan Winters	Teleperformance Group
Boris Wojtan	GSM Association
Kimon Zorbas	Nielsen