Centre for Information Policy Leadership
Hunton & Williams LLP

Accountability and Risk Management: Solutions for Enabling Effective Privacy Protection in Modern Information Age

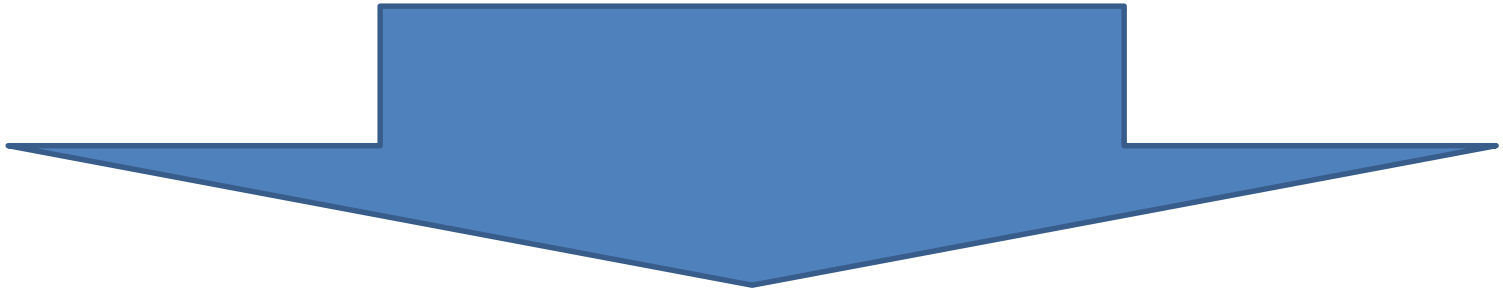
21 June 2016

Bojana Bellamy
President
Centre for Information Policy Leadership

Accountability in GDPR – Privacy Programme

Controllers must:

- Be responsible for compliance with GDPR
- Implement appropriate and effective technical and organisational measures to comply with the GDPR
- Demonstrate compliance & effectiveness of the measures



Taking into account:

- The nature, scope, context, and purposes of the data processing
- The risk for individuals - physical, moral, material damages

Centre for Information Policy Leadership
Hunton & Williams LLP

Privacy Management Programme – Universal Elements

Centre for Information Policy Leadership
Hunton & Williams LLP

Accountability Measures Under GDPR

Internal privacy policies and procedures - compliance rules for DP principles and individual rights	Security policies	External transparency measures	Measures to implement Privacy by Design/Default
Maintaining internal records of processing	Keeping documentation and evidence - consent, legitimate interest, notices, PIA, processing agreements, breach response	Conducting Privacy Impact Assessments - for high risk processing	Processor choice and management
Documenting and notifying personal data breaches - to the DPA and individuals	Maintaining transfer mechanisms for global data transfers	Appointing a DP Officer, with independent status, protected employment and statutory responsibilities	Co-operating with DPAs, on request

Centre for Information Policy Leadership
Hunton & Williams LLP

Demonstrating Accountability under GDPR

Accountability can be demonstrated via:

- BCR
- Approved Codes of Conduct
- Approved certifications
- Seals?
- Other accountability frameworks – e.g. ISO Cloud Privacy and Security Standard?

Risk Based Approach in GDPR

Horizontal – Accountability Obligation

- More flexibility for controllers to build, implement and demonstrate privacy programme and compliance measures, including tasks of DPOs
- Based on **likelihood and severity of risks for individuals**
- Based on nature, scope, context and purposes of processing

Specific obligations based on risk

- Privacy by design
- Data security
- Security breach notification to DPAs
- Appointment of representative of controller or processor established outside the EU

Specific requirements only for high risk processing

- Security breach notification to individuals
- Data Protection Impact Assessment
- Prior consultation with DPAs for high risk processing that cannot be mitigated

Implied consideration of risk

- Fair processing
- Legitimate interest balancing test
- Purpose limitation - determining compatibility of subsequent purposes

Further guidance provided by DPAs, EDPB, codes of conduct and certifications, DPO

Centre for Information Policy Leadership
Hunton & Williams LLP

Definition of Risk in GDPR

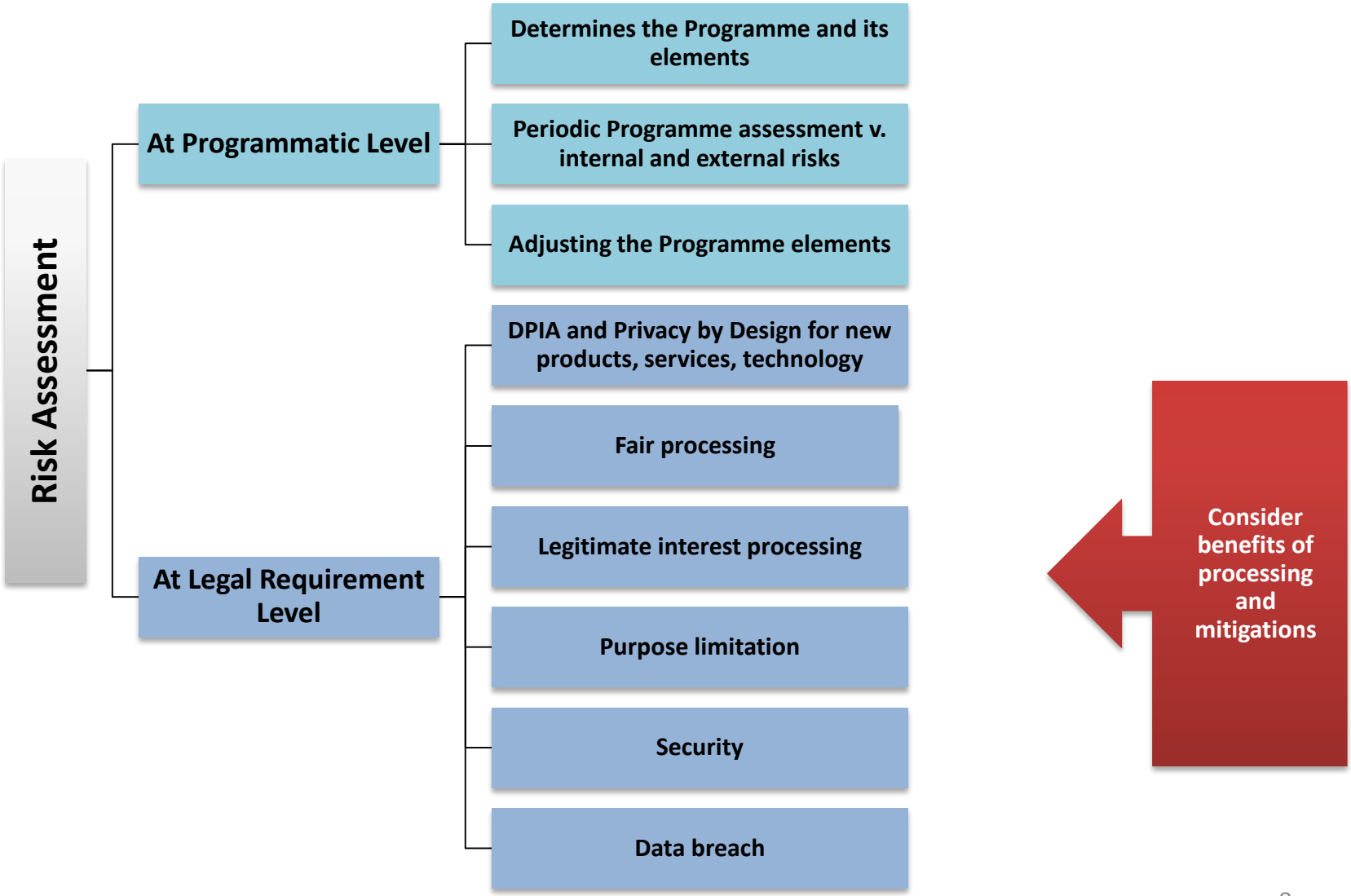
1. Personal data processing that may result in **physical, material or non-material damage**, in particular:
   - Discrimination
   - Identity theft / fraud, financial loss
   - Reputation damage
   - Loss of confidentiality of personal data protection by professional secrecy
   - Unauthorized reversal of pseudonymisation
   - Any other significant economic or social disadvantage
   - Individuals deprived of rights and freedoms, or prevented from exercising control over their data
   - Processing sensitive data, including genetic data
   - Profiling (personal aspects are evaluated (e.g. analyse or predict work performance, economic situation, health, personal preferences, behaviour, location) to create or use personal profiles
   - Processing children's and vulnerable persons' data
   - Processing large amounts of data and individuals

2. High risk

- High likelihood or severity of risks above, or involve use of new technology, or no DPIA carried out before, or time elapsed since initial processing

- Pre-defined types of high-risk processing – systematic automated decision taking; large scale processing of sensitive data or criminal convictions; systematic monitoring of public areas

Detailed View of Risk Assessments in the Context of Organizational Privacy Compliance Programs



Centre for Information Policy Leadership
Hunton & Williams LLP

In conclusion

- Organisational accountability – Corporate Digital Responsibility - is a corner-stone of effective privacy protection for individuals in modern information age and should be incentivised by DPAs – explicit in GDPR

- Risk management is critical to understand and address the impact on and potential harms to individuals – explicit in GDPR

- Understanding benefits to organisations, individuals and society is part of risk assessment and ethical decision making (judgement call) – implicit in GDPR?

- Ethical decision making is not an additional requirement, but already embedded in many GDPR requirements and an integral part of a judgement call when implementing GDPR requirements – implicit in GDPR?

- Risk based approach to supervision, enforcement should be an integral part of "smart regulation" and "smart DPAs".

Thank you

Bojana Bellamy
bbellamy@hunton.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton & Williams Privacy and Information Security Law Blog
www.huntonprivacyblog.com

FOLLOW US ON LinkedIn
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL