Robert Bond – Partner, Commercial/IP/IT

- **BA (Hons) Law, Wolverhampton University**
- **Qualified as a Solicitor 1979**
- **Qualified as a Notary Public 1989**
- **Companion of the British Computer Society**
- **Certified Compliance & Ethics Professional**

Robert Bond has nearly 40 years' experience in advising national and international clients on all of their technology, data protection and information security law requirements. He is a recognised legal expert and author in the fields of IT, e-commerce, computer games, media and publishing, data protection, information security and cyber risks.

He is Chairman of the Data Protection Network, Trustee of the UK Safer Internet Centre, a member of the Data Privacy Advisory Group to the United Nations, a member of the Board of TAPESTRY (Trust, Authentication and Privacy over a DeCentralised Social Registry) and is an Ambassador for Privacy by Design.

Experience

- Assisting clients in the financial services, life sciences, technology and retail sectors on a range of international regulatory and compliance issues
- Advising major medical device and pharmaceutical multinationals on data incidents
- Negotiating and drafting technology contracts for large and medium sized providers with customers.
- Acting for numerous multinationals on GDPR and global data protection compliance issues.
- Representing digital media companies as well as computer games companies on a range of commercial and online matters.

2

40 YEARS AGO WE DIDN'T HAVE…


Telex


eMail


Internet


Mobiles


Fax


Big Data


Social Media


Tablets


IoT


AI


Cloud


Websites


Drones


Blogs


CAV


Smart Cities

Data Protection Impact Assessment (DPIA)

What and Why?

DPIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information
Not mandatory, but 'promotes good practise'
DPIA identifies privacy risks and improves transparency
Projects that may require DPIA:

- A new IT system for storing and accessing personal data;
- Using existing data for a new and unexpected purpose;
- A new database acquisition
- Corporate restructuring
- Monitoring in the workplace

4

A right to know and assess privacy impacts

- People have a right to know if new technologies or services will intrude upon their privacy and human rights
- just as they have a right to know about the quality of the water they drink
- or the impact upon the environment of a new chemical production factory.

Trilateral Research & Consulting 2013

(EU PIA Framework)

5

What is a DPIA?

- a *process* for assessing the impacts on privacy of a project, technology, service, policy or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts.

- A PIA is about identifying risks and finding solutions, not simply producing a report that demonstrates compliance.

Trilateral Research & Consulting 2013

(EU PIA Framework)

6

ICO Guidance on PIA

- Way of complying with data protection obligations
- Method of Good Practice
- Can reduce costs
- Publish where appropriate
- Promotes trust

ISO 22307:2008

1. recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool to be used within an organization, or by "contracted" third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems.

The General Data Protection Regulation

Data Protection Impact Assessments and Prior Consultations (Articles 33)

- Required where 'using new technologies' and where potentially high risks for individuals' privacy rights
- DPO to consult with DPA where risks are particularly high

9

The General Data Protection Regulation

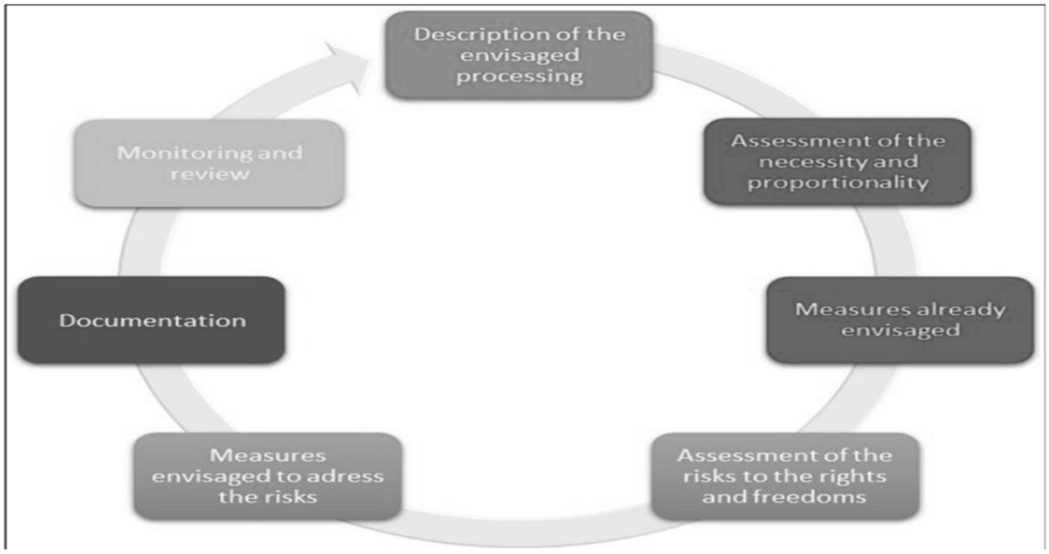
Privacy impact assessments

- DPIAs will become mandatory in the following cases:
  - A systematic and extensive evaluation of personal aspects of natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects on the individual or similarly affect the individual
  - Processing on a large scale of special categories of data or data relating to criminal offences
  - A systematic monitoring of publicly accessible areas on a large scale
- **DPAs will publish a list of when a DPIA is required or not required**

10

Data Protection Impact Assessment (DPIA)

WP29 Guidance



11

DPIA process

1. • Identify need for a DPIA
2. • Describe information flows
3. • Identify privacy risks
4. • Identify privacy solutions
5. • Record PIA outcomes, and sign-off
6. • Integrate PIA outcomes into project plan

DPIA process

1. **Identify need for a DPIA**
2. Describe information flows
3. Identify privacy risks
4. Identify privacy solutions
5. Record DPIA outcomes, and sign-off
6. Integrate DPIA outcomes into project plan

Identify need for a DPIA

1. What does the project or action hope to achieve?
2. Will new personal data be processed?
3. What choice will individuals have regarding their data?
4. Will human rights be impacted?
5. How intrusive will the technology be?
6. Is the processing of data proportionate?
7. Will the project have the potential to disadvantage individuals?
8. If you conclude no DPIA is necessary, explain why!

DPIA process

1. Identify need for a DPIA
2. **Describe information flows**
3. Identify privacy risks
4. Identify privacy solutions
5. Record DPIA outcomes, and sign-off
6. Integrate DPIA outcomes into project plan

16

Describe information flows

1. How will information be obtained, used and retained
2. Identify potential “function creep” – more use of personal data than might be expected
3. Ensure all people using such data focus on the practical implications
4. How, what, when, where and why will personal data be processed?

DPIA process

1. Identify need for a DPIA
2. Describe information flows
3. **Identify privacy risks**
4. Identify privacy solutions
5. Record DPIA outcomes, and sign-off
6. Integrate DPIA outcomes into project plan

Identify privacy risks

1. Record the risks to individuals, including privacy intrusion
2. Assess corporate and reputational risks
3. Conduct a compliance audit against applicable laws and regulations
4. Maintain a record of the identified risks

DPIA process

1. Identify need for a DPIA
2. Describe information flows
3. Identify privacy risks
4. **Identify privacy solutions**
5. Record DPIA outcomes, and sign-off
6. Integrate DPIA outcomes into project plan

Identify privacy solutions

- Devise ways to eliminate privacy risks
- Assess the costs and benefits of each solution
- Consider how each solution reduces privacy risks
- Consider how each solution impacts upon the project

DPIA process

1. Identify need for a DPIA
2. Describe information flows
3. Identify privacy risks
4. Identify privacy solutions
5. **Record DPIA outcomes, and sign-off**
6. Integrate DPIA outcomes into project plan

Record DPIA outcomes, and sign-off

1. Record the outcome of the DPIA and the methodology used
2. Obtain sign-off from an authorised officer
3. Make the DPIA Report available as necessary to key stakeholders

PIA process

1. • Identify need for a DPIA
2. • Describe information flows
3. • Identify privacy risks
4. • Identify privacy solutions
5. • Record DPIA outcomes, and sign-off
6. • **Integrate DPIA outcomes into project plan**

Integrate DPIA outcomes back into the project

1. Ensure that the outcomes of the DPIA Report are implemented
2. Ensure that the DPIA is a “living document” and is consulted during the lifecycle of the project
3. Integrate any lessons learned from the DPIA into a DPIA Policy and Handbook

DPIA Policy and Handbook

1. Create a Policy
2. Create a Handbook
3. Train and train again!

How to make legitimate interests "legitimate"?

How to make legitimate interests “legitimate”
Guidance on the use of Legitimate Interests under GDPR

- EU Data Protection Directive (95/46/EC) includes “Legitimate Interests” as a lawful ground for processing
- EU General Data Protection Regulation sets out 6 lawful grounds for for processing, of which Legitimate Interests is one

Under Article 6 1(f)
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child.

Under Recital 47
The legitimate interests of a controller, including those of a controller to which the Personal Data may be disclosed, or of a Third Party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

27

How to make legitimate interests “legitimate”
Guidance on the use of Legitimate Interests under GDPR

- Processing needs a legal basis

✓ Consent

✓ Contractual

✓ Legal obligation

✓ Vital interests

✓ Public task

✓ Legitimate interests

◆ There is no hierarchy of grounds for lawful processing, but

◆ Different legal grounds carry different duties

◆ Controllers must be transparent about which basis they rely upon

28

How to make legitimate interests “legitimate”

Guidance on the use of Legitimate Interests under GDPR

Recitals 47 to 50 in the GDPR give some examples of when a Controller may be able to rely on Legitimate Interests:
1) DIRECT MARKETING - processing for direct marketing purposes under Legitimate Interests is specifically mentioned in the last sentence of Recital 47.
2) REASONABLE EXPECTATIONS - where individuals have a reasonable expectation that the Controller will process their Personal Data, subject to the balancing test.
3) RELEVANT & APPROPRIATE RELATIONSHIP - where there is a relevant and appropriate relationship between the individual and the Controller in situations where the individual is a client or in the service of the organisation. Examples of this would include (i) if an individual had recently (within the last 2 years) purchased goods or services from the Controller or donated to an organisation (ii) where the individual was a member of staff of the Controller.
4) STRICTLY NECESSARY FOR FRAUD PREVENTION - where the processing is strictly necessary for the purpose of preventing fraud. This could include verifying the registered address of the cardholder for a particular credit or debit card is the same as the cardholder’s normal place of residence or work.
5) ORGANISATIONAL - where Controllers that are part of an organisational group or institutions affiliated to a central body transmit Personal Data within that organisational group or to the central body. However, the rules on transferring Personal Data to a country outside Europe must be complied with if this is relevant.
6) NETWORK & INFORMATION SECURITY - where the processing of Personal Data is strictly necessary and proportionate for the purposes of ensuring network and information security. An example of this would include monitoring authorised users’ access to a Controller’s computer network for the purpose of preventing cyber-attacks.

29

How to make legitimate interests “legitimate”

Guidance on the use of Legitimate Interests under GDPR

- If a Controller wishes to rely on Legitimate Interests for processing Personal Data it must carry out an appropriate assessment, which we have called a Legitimate Interests Assessment, or LIA.
- When carrying out an assessment, the Controller must balance its right to process the Personal Data against the individuals’ data protection rights.
- In certain circumstances an LIA may be straight forward. However, under the accountability provisions of the GDPR, the Controller must maintain a written record that it has carried out an LIA and the reasons why it came to the conclusion that the balancing test was met.
- Legitimate Interests may be considered where:

✓ another legal basis is not available due to the nature and/or scope of the proposed processing; or
✓ where there are a number of legal bases that could be used but Legitimate Interests is the most appropriate.

30

Questions?

Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44(0)20 7400 8000