Data Protection

Managing Information Privacy

Trainer: Paula Williams

1

Course Content

- What is information privacy
- Why is information privacy important
- Identify and manage privacy risk
- Data Protection Impact Assessment
- Information privacy failures

2

What is Considered Personal Data?

Personal Data

Any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly.

The definition of personal data has been increased to include location data (GPS), genetic data e.g. biometrics, online identifiers (IP addresses) and social identifiers e.g. religion.

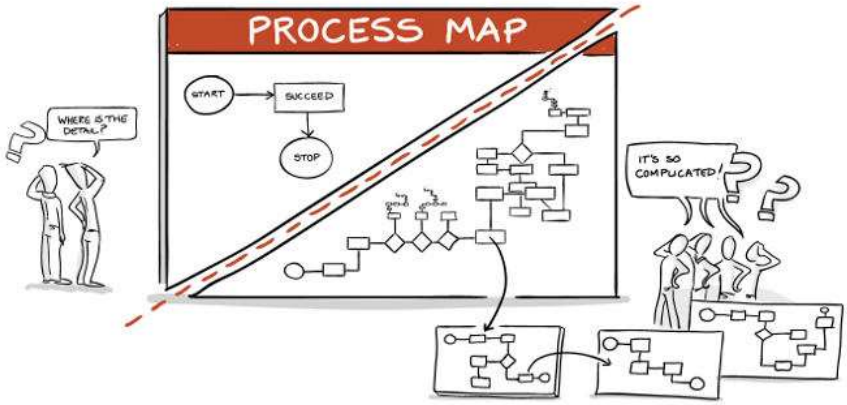
Sensitive Personal Data

Is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sexual information, criminal proceedings or convictions.

Also Includes: *Opinions, Files, Old Databases, Back ups, Data Combinations, CCTV*

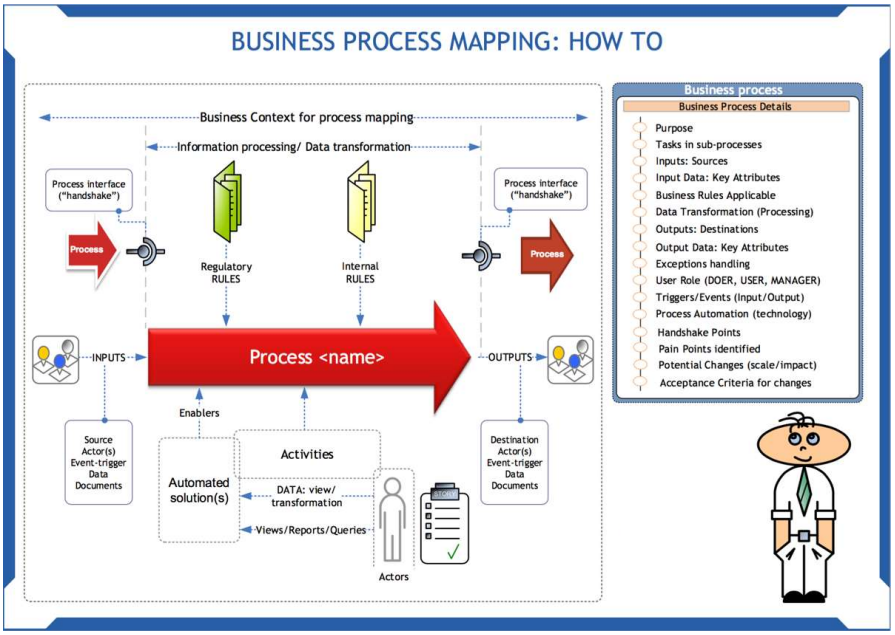
Data Process Mapping

For Large or More Complex Businesses: Once you understand what data you hold **(Data Audit)** you will require a **process map** to understand how the data is being used across the company.



Data Process Mapping

Handout One



What is Privacy?

Individuals Right to be left alone

1. **Physical -** the ability of a person to maintain their own physical space or solitude

2. **Information -** the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others

What would be intrusive to an individuals privacy?

What is Privacy by Design?

Companies require a **structured and methodical approach to assessing the risks**

By identifying and addressing potential problems at an early stage:

- easier and more cost-effective than addressing issues later
- increased awareness of privacy and data protection
- company's actions be less privacy intrusive (reduced impact on individuals)
- reduced risk of Data Protection Act breach

Privacy by Design – Founding Principles

1. Proactive & Preventative
2. Privacy as a Default Setting
3. Privacy is embedded into Design
4. Full Functionality – 'Win-Win' Approach
5. End-to-End Data Lifecycle Protection
6. Visibility and Transparency
7. Respect for Privacy – 'User-Centric'

Why Privacy by Design?

Handout Two

Risk of Harm or Distress from an Intrusion into Privacy

Common Information Risks:

- Too much information
- Insecure information
- Inaccessible information
- Incorrect information
- Information-sharing for new purposes

The internet makes it possible to piece together a picture of individuals private lives.

Managing the Impact of Change

Privacy management requires that you consider:

- the level of the possible harm, or likelihood of harm to individual
- whether the change is consistent with what individuals would expect you to do.

When might I need to think about privacy?	
• New IT system	New surveillance system
• Outsourcing a service/process	New way of storing Information
• Data sharing initiative	New Policies or strategies
• Using personal data in a new way	To assess existing systems

Tools: Brief Privacy Analysis and a Privacy Impact Assessment

Privacy Impact Assessment

Systematic process for evaluating a process or change in terms of its impact on privacy

PIA will help to:

- identify a positive or negative impact
- check compliance with privacy laws
- help to manage any privacy risks
- maximise the benefits of protecting privacy well
- be as a reference point for future actions

When a PIA is Not Needed

Use of the personal information might be uncontroversial:

- level of the possible **harm**, or the likelihood that the harm will in fact occur, might be **negligible**
- change to how the information is managed is **minor** and is **consistent** with what the individuals concerned would expect you to do.

Guiding Principles for Managing Personal Information

During the lifecycle of that information *(from collecting it to destroying it):*

1. Only collect personal information if you really need it
2. Get information from person concerned or check accuracy from 3rd party if needs be.
3. Tell them what you're going to do with their data
4. Be fair and not unreasonably intrusive when you're getting data
5. Keep their information safe
6. Give people access to their personal information if they want it

13

Guiding Principles for Managing Personal Information

7. Let people correct information that's wrong
8. Make sure personal information is correct and not misleading before you use it
9. Get rid of it when you're done with it
10. Generally, only use the information for the purpose for which you got it
11. Only disclose it if you have a good reason
12. Only assign unique identifiers where permitted.

14

Scenario: Your company sells gift products and are looking at extending to online sales. Your current website is relatively basic and does not list products or allow for purchases online at the moment.

Operationally, this is a move away from selling direct to the customer from your shop floor.

15

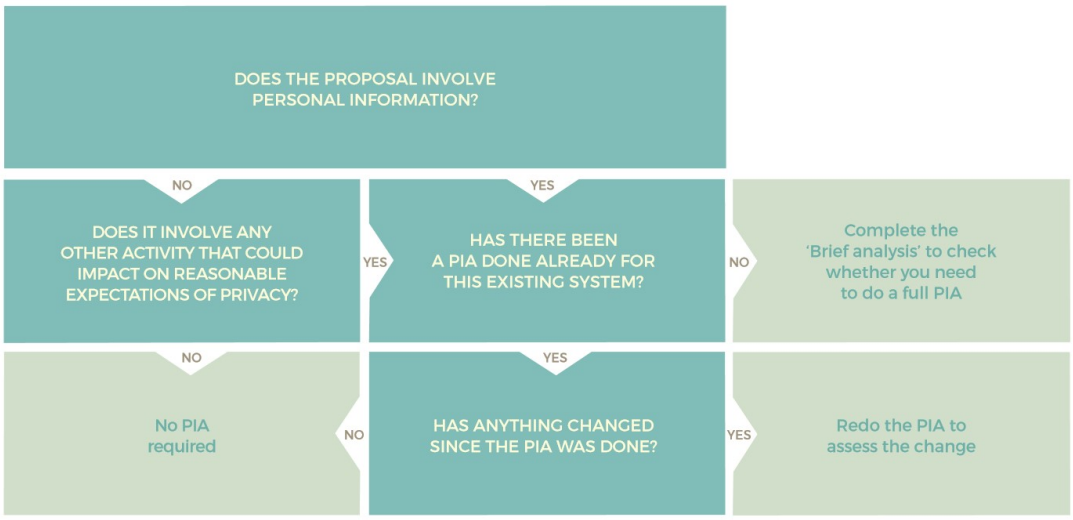
Scenario: Your company sells gift products and are looking at extending to online sales. Your current website is relatively basic and does not list products or allow for purchases online at the moment.

Operationally, this is a move away from selling direct to the customer from your shop floor.

Step One: Consider the above scenario and look at the following slide to see if we need to be thinking about undertaking a BPA or PIA?

16

First Check …



17

Handout 3 & 4

Scenario: Your company sells gift products and are looking at extending to online sales. Your current website is relatively basic and does not list products or allow for purchases online at the moment.

Operationally, this is a move away from selling direct to the customer from your shop floor.

Step One: Consider the above scenario and look at the following slide to see if we need to be thinking about undertaking a BPA or PIA?

Step Two: Complete a Brief Privacy Analysis using the 'Risk' Checklist to assess whether a full Privacy Impact Assessment is required.

18

Handout Five

Scenario: Your company sells gift products and are looking at extending to online sales. Your current website is relatively basic and does not list products or allow for purchases online at the moment.

Operationally, this is a move away from selling direct to the customer from your shop floor.

Step One: Consider the above scenario and look at the following slide to see if we need to be thinking about undertaking a BPA or PIA?

Step Two: Complete a Brief Privacy Analysis using the 'Risk' Checklist to assess whether a full Privacy Impact Assessment is required.

Step Three: Undertake a full Privacy Impact Assessment.

island CONSORTIUM

19

More Complex Privacy Impact Assessments

- Get an external view of your PIA
- Consult with stakeholders
- Establish better governance structures to manage personal information
- Manage any risks with using third-party contractors
- Align the PIA with the organisation's existing project-management methodologies
- Publish your PIA

island CONSORTIUM

20

Data Privacy Failures

Doorstep Dispensaree - left 500,000 documents in unlocked containers at the back of its premises, which included names, addresses, dates of birth, NHS numbers, medical information and prescriptions without appropriate protection and were subsequently water damaged. **(£250k)**

Taxa 4x35 – Copenhagen taxi company anonymised personal data but not telephone numbers – kept more 3 years after deletion date. Anonymising data is hard to achieve in practice, consider pseudonymising data. **(EURO 161k)**

Shell - Former employee emailed a database with the contact details of 170,000 Shell workers to campaigning groups. Prevention is important – access controls preventing large downloads of data.

Data Privacy Failures

Hudson Bay Finance – Not responding to a Subject Access Request. Train all staff to recognise a SAR and respond accordingly, have an external company test the protocols to ensure your policies and procedures work. SARs are often connected with a complaint or a concern.

Second Hand IT – Over 6 months, a security researcher found thousands of files from dozens of computers, phones and flash drives, most of which contained personal data from their previous owners. Organisations remain responsible for the personal data they control, no matter who owns the hardware that stores it.

North American Casino - Fish tank sensors connected to a PC that regulated the temperature, food and cleanliness of the tank was used to move into the network and send out data. IoT technology is vulnerable to being hacked or compromised.

This publication has been prepared for general guidance on matters of interest only, and does not constitute legal advice.

No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication. Island Consortium does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.