



Achieving GDPR Compliance Guide – The Last 10 Steps Analysed

Ray Thorpe

Senior Manager, Information Governance



**INVESTORS
IN PEOPLE**



Webinar Objectives

1. Introduction to BSI Cybersecurity and Information Resilience.
2. GDPR; what is it and what do I have to do?
3. A sequential and prioritized approach – the last 10 steps to compliance (Operational [6] and Communicative [4]).
4. Provide enough information to bring back to your organisations to further the conversation.

**Through the passion and expertise
of our people, BSI embeds
excellence in organizations across
the globe to improve business
performance and resilience.**

Cybersecurity and Information Resilience – what we do

We enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

bsi.



What do we do?



Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services.



Security awareness

Phishing and user awareness training, SaaS solutions, social engineering and simulation testing



Data management and privacy

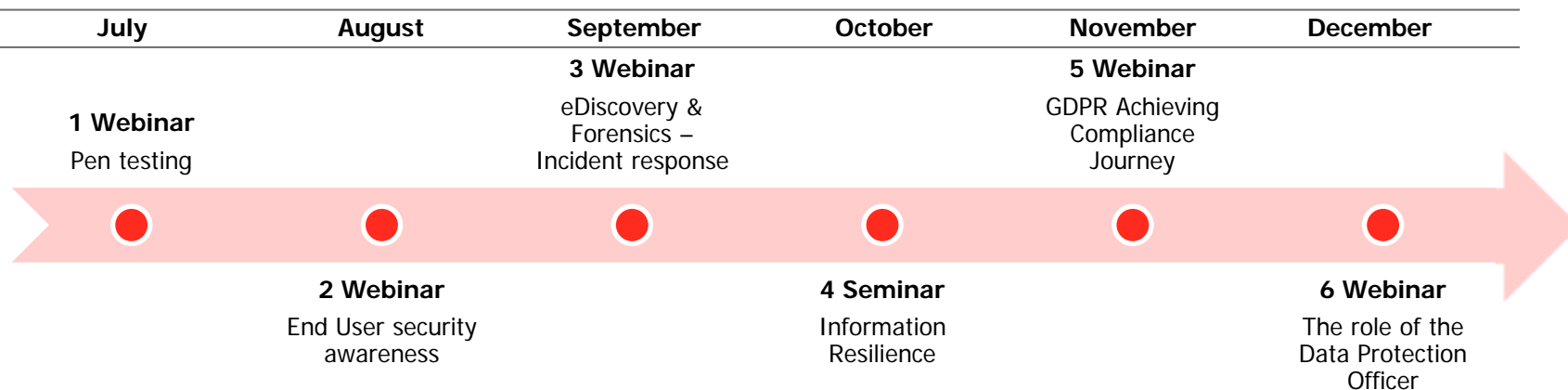
GDPR services, information lifecycle management and eDiscovery and forensics



Compliance and testing

PCI DSS services, cyber lab testing and product and software assessments (CC, CAS-T/CPA)

Path to GDPR – Cybersecurity and Information Resilience Services



Webinar Series:

1. **Penetration Testing (Jul17)** – ensuring an organization's customer and prospect data is secure
2. **End User Security Awareness (Aug17)** – Untrained employees - the weakest link in your cybersecurity defence
3. **Incident Response (Sept17)** – You have 72 hours to respond after a breach... was personal data compromised?
4. **Information Resilience Series Event (Oct17)** – Manchester 17th October 2017
5. **GDPR Achieving Compliance Journey (Nov17)** – a step-by-step methodology for achieving compliance
6. **GDPR – the role of the Data Protection Officer (Dec17)** – Is your organization's DPO ready?
7. **Achieving GDPR Compliance Guide (Mar17)** – The first 10 steps Analysed

BSI GDPR Compliance Professional Services

Understanding

GDPR foundation training course

One day training course

We help you understand the fundamentals of GDPR

- Gain the confidence to interpret data protection regulations
- Learn to integrate GDPR policies and procedures

Scoping workshop

Stakeholder engagement

We identify relevant information, activities and controls

- Compile inventories of Personally Identifiable Information (PII)
- Identify data flows and data processors
- Confirmation of regulatory requirements

Implementation

Gap analysis

Identify gaps in compliance

We assist you to identify the critical areas in need of improvement

- Gap analysis against GDPR requirements
- Verification assessment
- Audit against privacy standards eg. BS 10012, ISO 29000

Implementation support

Implement the key principles of GDPR

We help you establish the necessary policies and procedures

- Outsourced Data Protection Officer (DPO) services
- Data breach reporting
- Privacy by design
- Completion of Privacy Impact Assessment
 - PACE Privacy Assessment and Coverage Engine (fully automated)

Validation

Compliance validation

Post-implementation assessments

We perform the necessary checks to ensure all gaps have been closed

- Internal audits
- Privacy compliance audits
- Third party and supply chain audits

Ongoing support

Continuous assessment and support

We offer a partner programme service for essential assistance

- Data breach/incident on-call support
- Subject access request support services
- Supervisory Authority audit support

The journey to GDPR compliance

General Data Protection Regulation in 1 Minute

- Aims to **protect** the personal data of EU citizens
- Puts individuals back in **control** of their personal data
- Applies to all EU member states, any organization who operates within the EU market, or who holds information on EU data subjects
- Requirement to **report** a data breach to the data protection commissioner, within 72 hours of becoming aware of any breach
- **Fines** of up to €20 million or up to 4% of annual worldwide turnover for non-compliance (whichever is **higher**)
- Comes into force on the **25th May 2018**
- Data Protection Officer (DPO) appointment
- No opt out for UK with **Brexit**



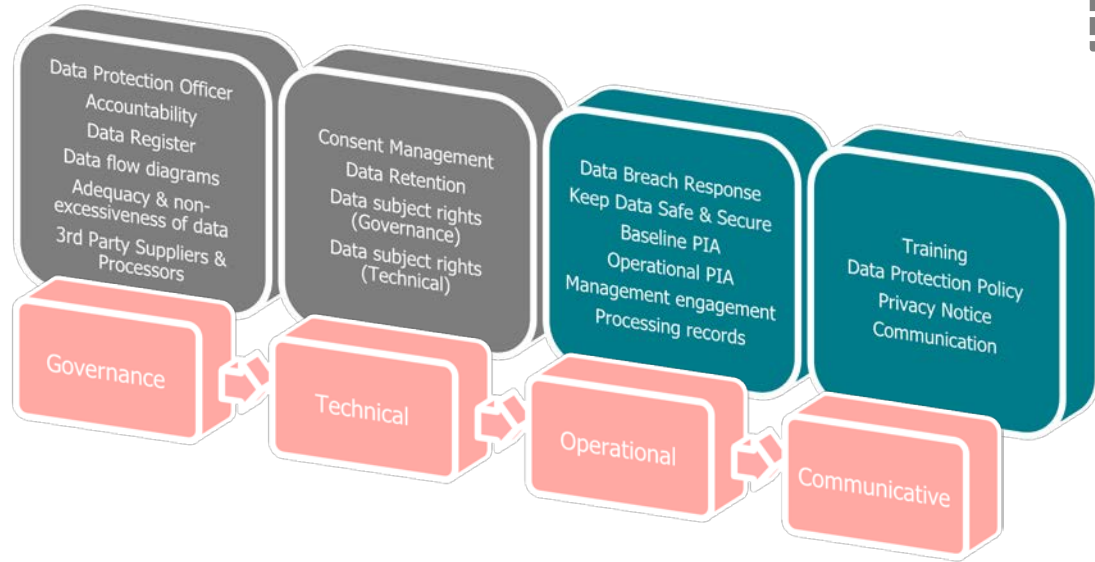
20 Steps to GDPR Compliance

- What you need to do, in a prioritised manner...

20 Steps to Compliance

Webinar #10:
the next 10 of the
20 steps analysed

Webinar #9:
the first 10 of 20
steps analysed



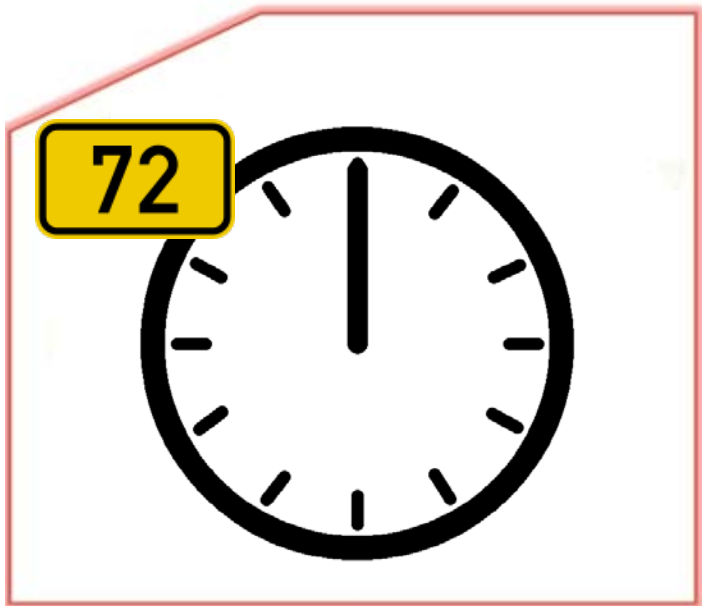
The Last 10 Steps

11. Data Breach Response
12. Keep Data Safe and Secure
13. Baseline PIA
14. Operational PIA
15. Management Engagement
16. Processing Records
17. Training
18. Data Protection Policy
19. Privacy Notice
20. Communication

Step 11: Data Breach Response

Operational

- Understanding Breach Response Requirements, Timelines and Notifications
- Agree and document data breach / data security incident response process
- What is a personal data breach?




72

Difficulty level: Low (Really?)

Step 11: Data Breach Response

Operational

- Understanding Breach Response Requirements - Timelines
 - Any real or suspected event that may involve the loss or disclosure of personal or sensitive personal data
 - Controllers must notify most data breaches to the Data Protection Authority (DPA)
 - “Where feasible” no later than 72 hours after the breach
 - Where there is a high risk to the data subject due to the breach, they must also be notified “without undue delay”
 - A reasoned justification must be provided if this timeframe is not met
- Exemptions



Difficulty level: Low (Really?)

Step 11: Data Breach Response

Operational

- Understanding Breach Response Requirements - Notifications
- Notifications and reports must contain:
 - Categories of data
 - Number of individuals
 - Records affected
 - DPO
 - Consequences
 - Mitigation measures

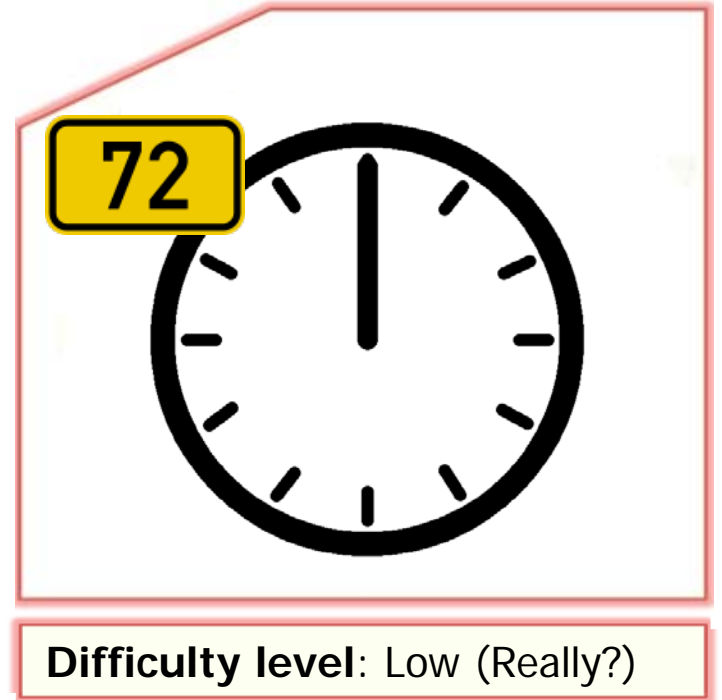
72

Difficulty level: Low (Really?)

Step 11: Data Breach Response



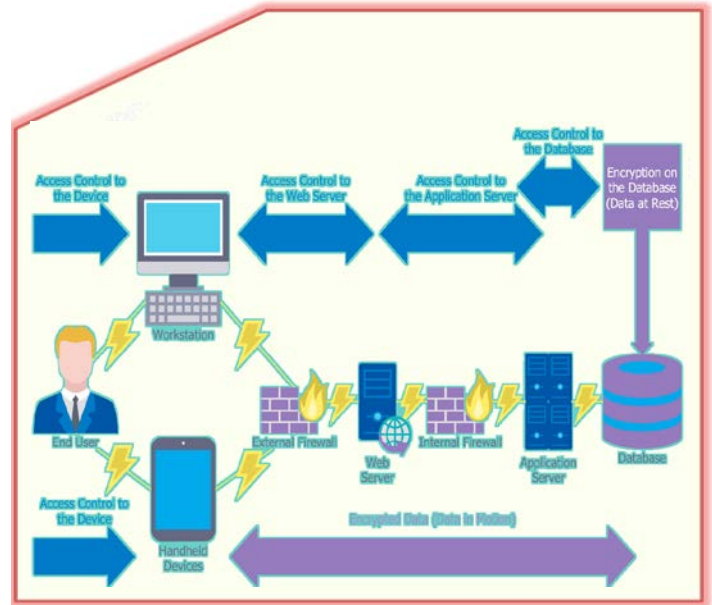
- Action:
 - Establish roles and responsibilities
 - Review data registers and flows
 - Document and agree a formal incident response plan
 - Test the plan regularly
 - Logging and alerting
 - Security/Incident response partner



Step 12: Keep Data Safe & Secure

Operational

- Article 32
 - Appropriate Security of Processing
- We can only secure what we understand
 - Data registers
 - Data flows
- Expected Security Controls

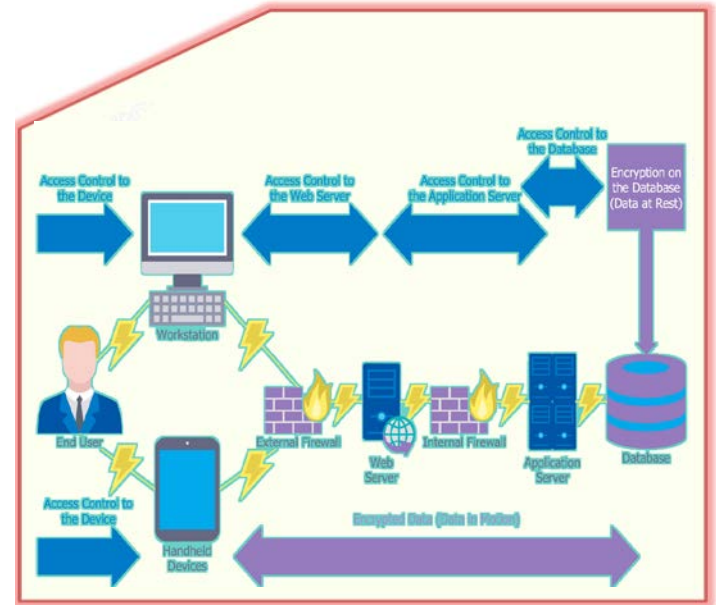


Difficulty level: Challenging

Step 12: Keep Data Safe & Secure

Operational

- Action:
 - Data discovery
 - Self assessment of security controls
 - Patch and vulnerability management frameworks
 - Regular independent assessments

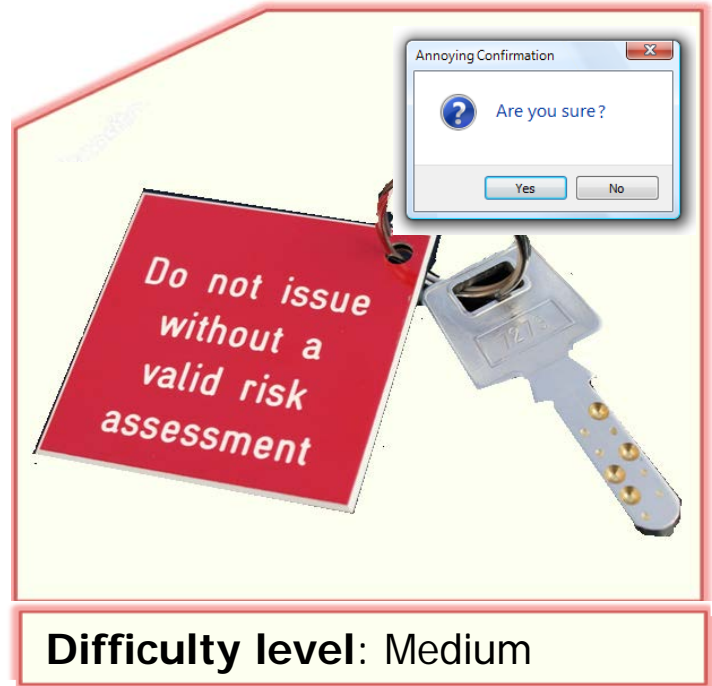


Difficulty level: Challenging

Step 13: Baseline PIA

Operational

- Privacy by design in practice.
- Complete baseline privacy impact assessment
- NOT a specific legal requirement under GDPR...
- BUT!
- What is a PIA made of?



Difficulty level: Medium

Step 13: Baseline PIA

Operational

| Inputs | Outputs |
|--|---|
| <ul style="list-style-type: none">• Information registers• Data flows• Policies/procedures• Processes<ul style="list-style-type: none">• Project management• Risk management• Compliance management | <ul style="list-style-type: none">• A minimization of privacy risk across the org• Informed risk decision making• Understanding of how to approach data protection.• Concrete understanding of how and why particular decisions are made about data• Transparent expectations of how subject data will be used and why• Feedback of risks to the project |

Step 14: Operational PIA



- Agree and document repeatable approach for ongoing privacy impact assessments.
- Embed PIA gateways into other processes i.e.
 - SDLC
 - Project Management
 - Change Management
 - Procurement
 - etc.



Step 15: Management engagement



- Management oversight is a legal requirement.
- Ensures:
 - Responsibility are clear and penalties understood
 - Driving of privacy/GDPR alignment
 - Effective and efficient regime



Difficulty level: Hmmmm...

Step 15: Management engagement



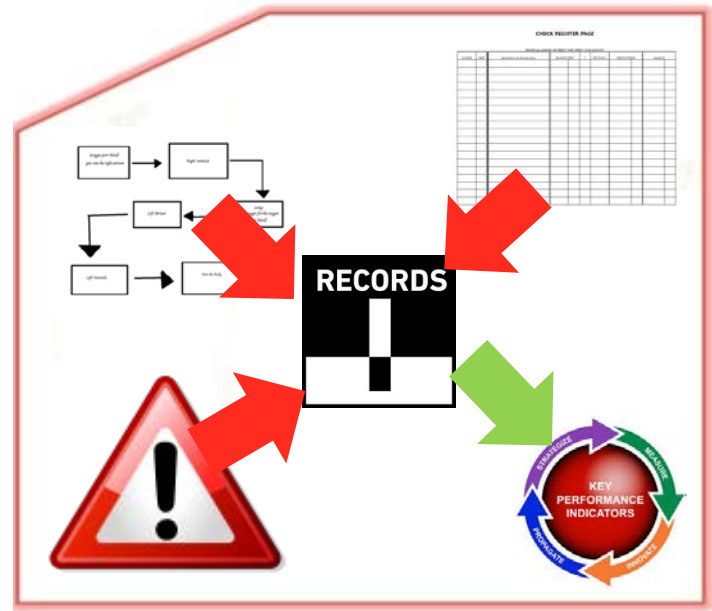
- Actions:
 - Appoint Data Protection Officer
 - Elect "Privacy Champions" throughout the organisation
 - Agree and present DP as a standing item at board meetings with relevant information / KPIs.
 - Privacy and compliance risk



Difficulty level: Hmmmm...

Step 16: Processing records

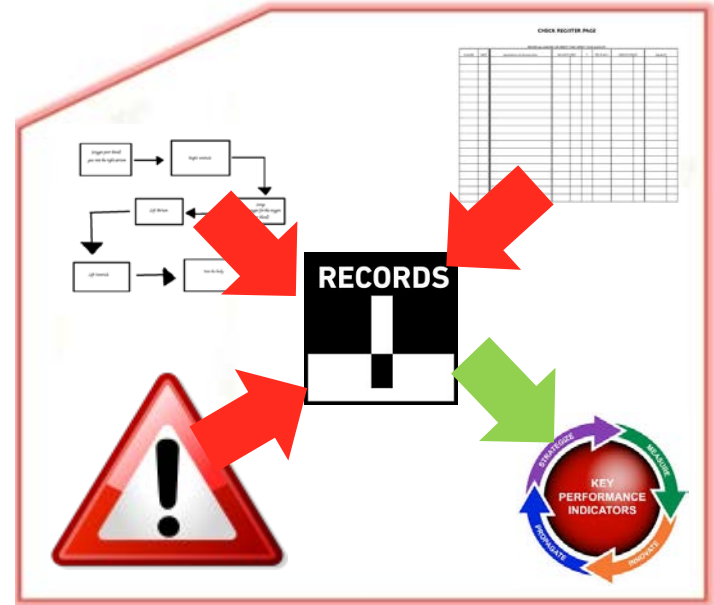
- Now a legal mandate to maintain detailed records of processing operations.
- Article 30
 - “Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.”
- What do we need to document under Article 30 (1) of the GDPR - if we are a controller?
 - Name and contact details of your organisation
 - Purpose of processing
 - Categories of individuals/data
 - Details of transfers to other countries and safeguards
 - Security measures in place to security the data being processed



Difficulty level: Low (Really?)

Step 16: Processing records

- Now a legal mandate to maintain detailed records of processing operations.
- Suggestion is that records should include at least the following:
 - Information register
 - Data Retention Register
 - Third Party Transfer Register
 - Subject access request register



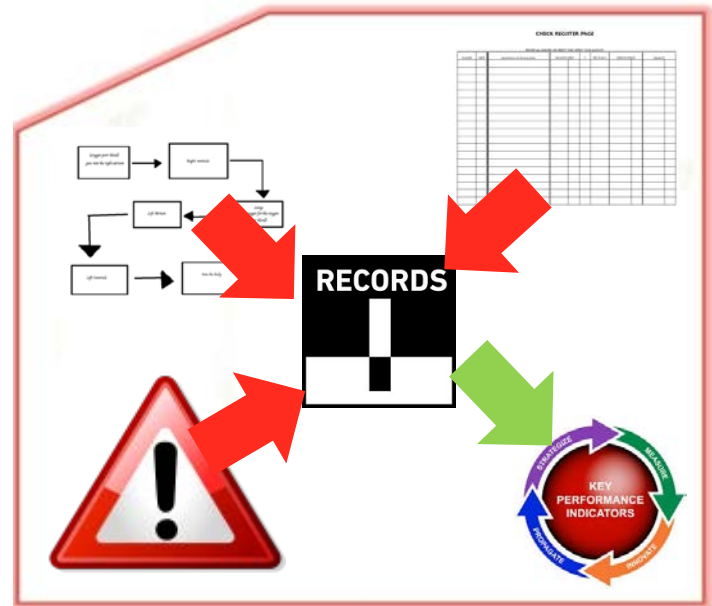
Difficulty level: Low (Really?)

Note: as per diagram...

Step 16: Processing records

Operational

- Action:
 - Coordinated project across the organisation
 - Correlate the data from data discovery

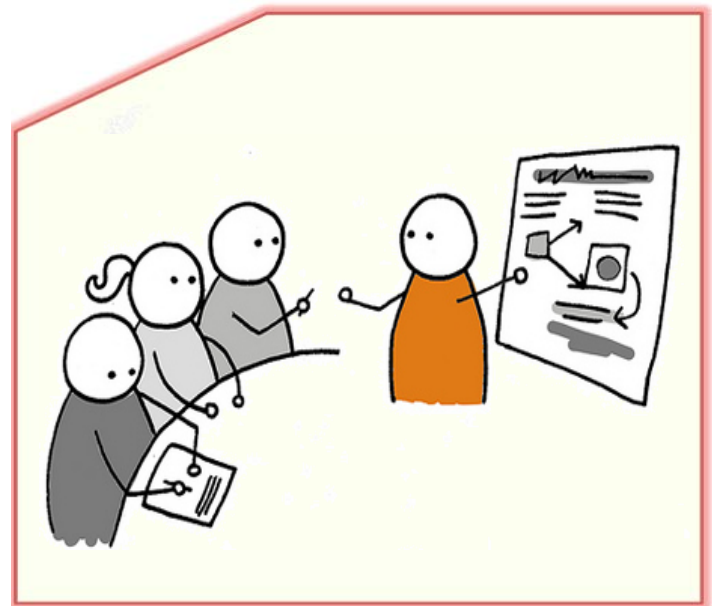


Difficulty level: Low (Really?)

Step 17: Training

Communicative

- Now a legal mandate to ensure that all staff who handle personal data receive appropriate training.
- Training to include:
 - Staff processing sensitive personal data will require tailored training
 - Staff should receive training at induction stage and before accessing personal data and should also receive annual refresher training
 - Maintain a Training Log
 - Third Party Processors!

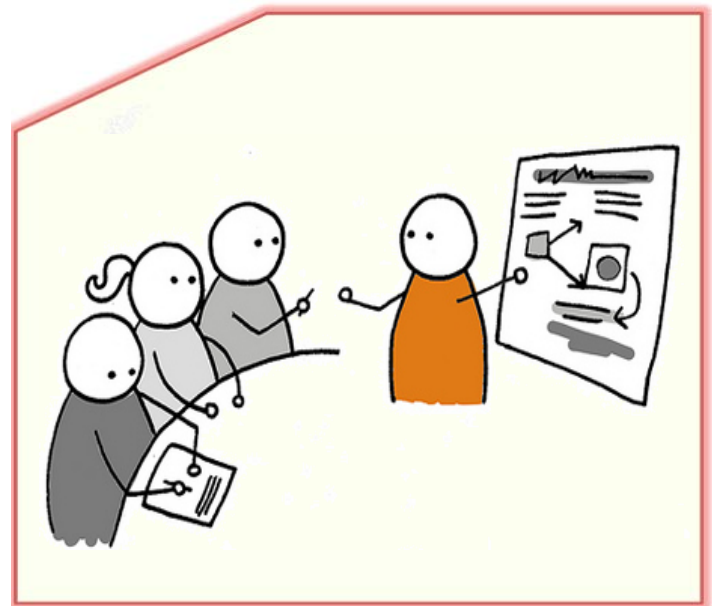


Difficulty level: Medium

Step 17: Training

Communicative

- Action:
 - Dedicated data protection and GDPR awareness
 - Onboarding
 - Regular awareness training
 - Specialised training
 - Document and manage training log



Difficulty level: Medium

Step 18: Data Protection Policy



- Critical
- Article 24
 - Under Article 24 of the GDPR, the Regulation states that *"[w]here proportionate in relation to processing activities, [...] measures [...] shall include the implementation of appropriate data protection policies by the controller."*
- Policy will establish:
 - Scope
 - Legal basis
 - Applicable principles/regulation
 - Roles and Responsibilities
 - Definite key terms

A graphic with a yellow background and a red border, shaped like a house. It contains the title "Data Protection policy" in blue and a list of 8 numbered points in black text. On the left side, there is a vertical label "Information" in a light blue font, and on the right side, there is a vertical label "Data" in a light blue font.

Data Protection policy

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Difficulty level: Medium

Step 18: Data Protection Policy



- Action:
 - Review existing data protection policy
 - If required draft a new policy to define:
 - Data categories
 - Terms
 - Responsibility
 - Rights of data subjects
 - Third parties
 - Data security measures
 - Integration with existing policu
 - Consequences

A graphic representing a document titled "Data Protection policy". The document has a yellow background and a red border. On the left side, there is a vertical label "Introduction" in a light blue font. On the right side, there is a small blue icon of a person. The main content is a list of 8 numbered points in black text.

Data Protection policy

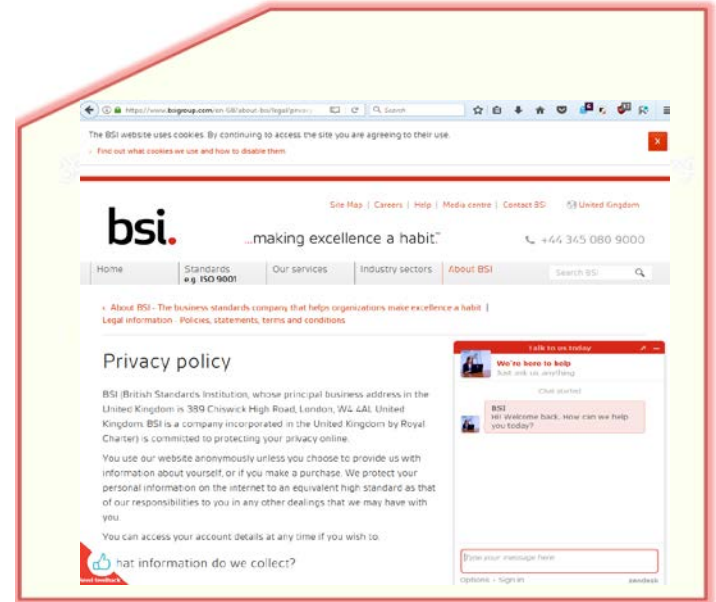
1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Difficulty level: Medium

Step 19: Privacy Notice



- Privacy Notice
 - Inform data subjects
 - Articles 12, 13, 14
 - Understandable and accessible
 - Transparent and concise
- What do we need to make clear to data subjects
 - Who
 - What
 - Why
 - Where
 - How

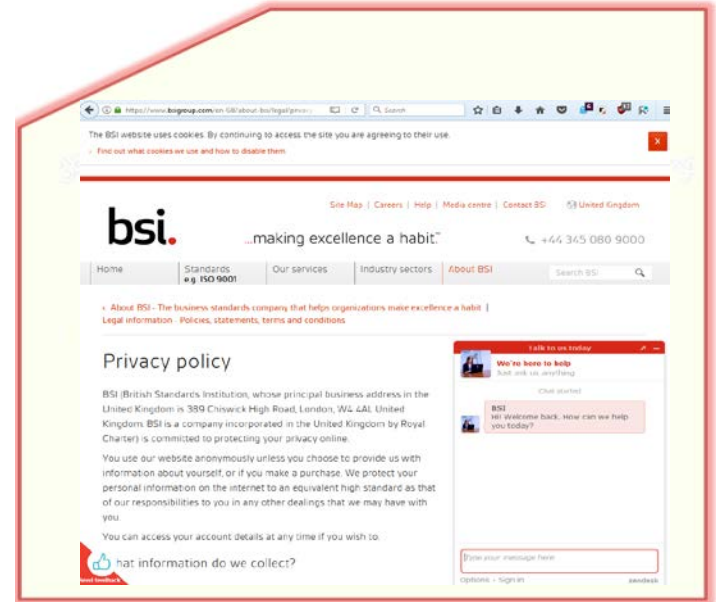


Difficulty level: High

Step 19: Privacy Notice



- Action:
 - Review business processes and existing privacy notices
 - Correlate with existing privacy framework documentation
 - Update data **privacy notice** to account for outputs of all the above processes.



Difficulty level: High

Step 20: Communication



- Publish and distribute updated DP policy and updated Privacy Notice to all appropriate stakeholders (internal and external)
- Be clear to all internal stakeholders: this is what we do and what our expectations are.
- Be clear to all **external** stakeholders:
 - This is the data we have
 - This is why we have it
 - This is what we do with it
 - This is where we store it
 - This is how long we'll hold it for
 - This is how you can exercise your rights



Difficulty level: Low (But...)

The Bad News

No one element will solve your problems

For compliance, you will need...

- Privacy Governance
- Defensible Position
- Structure Methodical Approach
- Specialist software
- Broad range of Experience
- Legal advice



The Good News

BSI Cybersecurity and Information Resilience consultants provide:

- GDPR Project Management ✓
- Specialist Consultancy Advice ✓
- Implementation Support ✓
- Specialist Software ✓
- DPIA and Policy Development ✓
- Experience with Supervisory Authorities ✓



BSI – Data Protection & GDPR Services

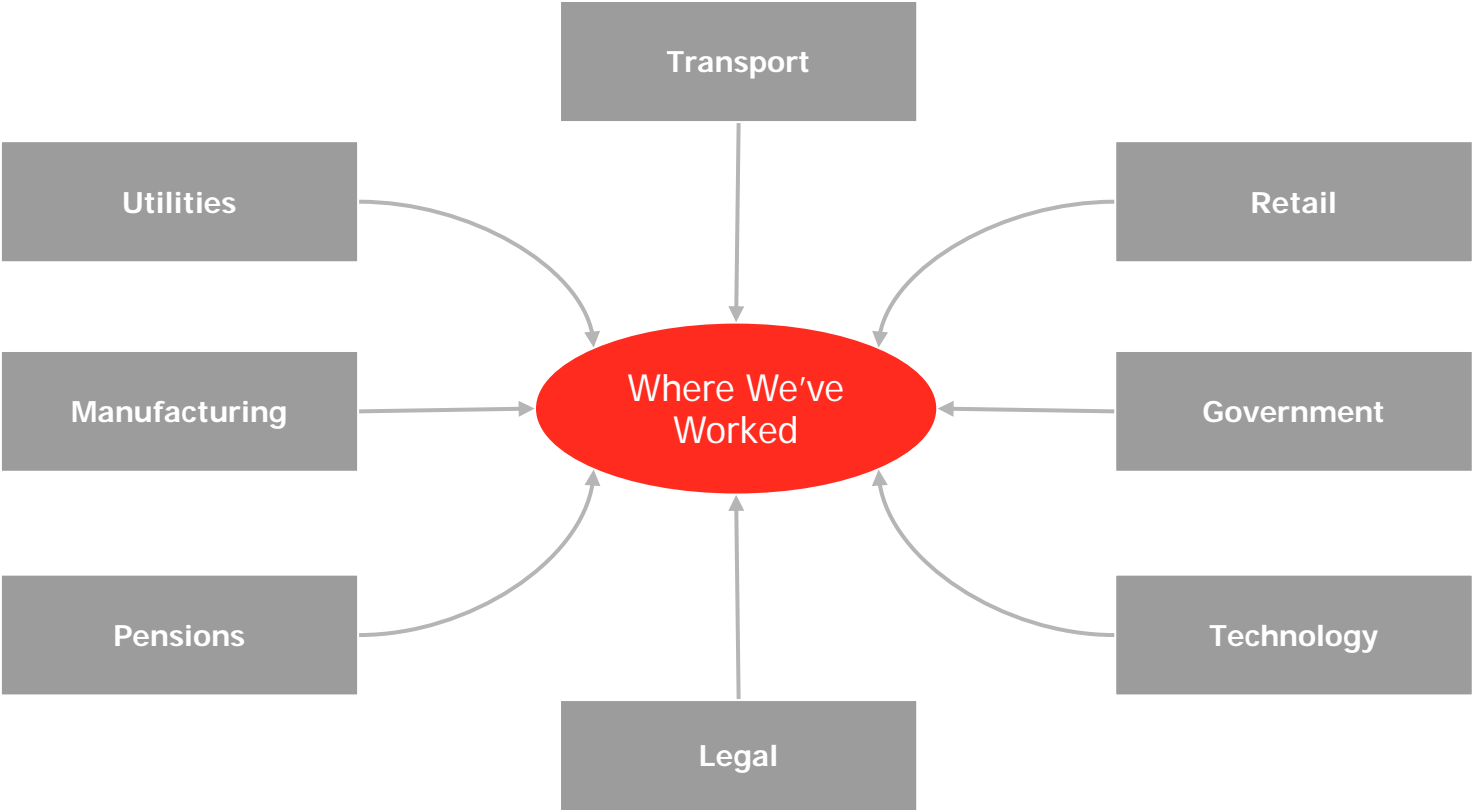
Information & Privacy Governance

- Data Protection Implementation Support
- Data Protection Officer (DPO) Services (Onsite and/or Virtual)
- Data Protection / Privacy Impact Assessments
- Data Protection Training
- Data Protection Audit Support (Internal and/or External)

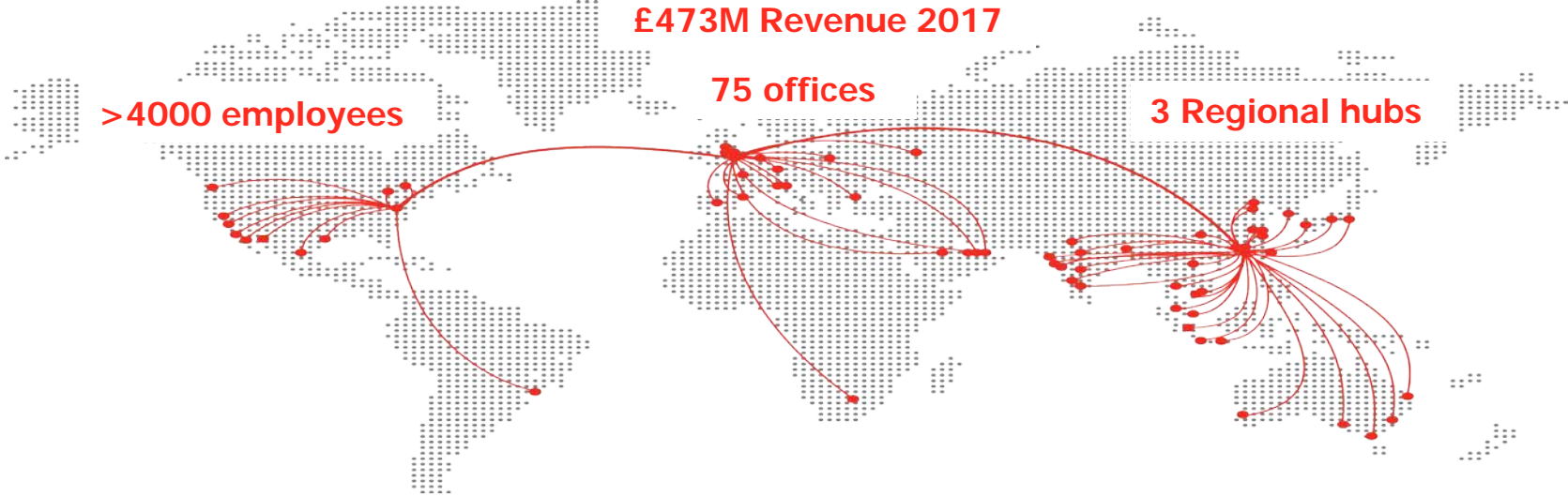
Technical Consulting

- Technical Penetration Testing & Vulnerability Management
- eDiscovery Support
- Data Breach Response and Digital Forensics

BSI – Where We've Worked



BSI – Where We Operate



Get In Touch

UK

Phone: (+44) 345 222 1711

Email: cyber@bsigroup.com

Global

Phone: (+353) 1 210 1711

Email: cyber.ie@bsigroup.com