Achieving GDPR Compliance Guide – The First 10 Steps Analysed

Stephen Scott

Senior Manager, Information Governance

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 first 10 steps to compliance (Governance [6] and Technical [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.

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

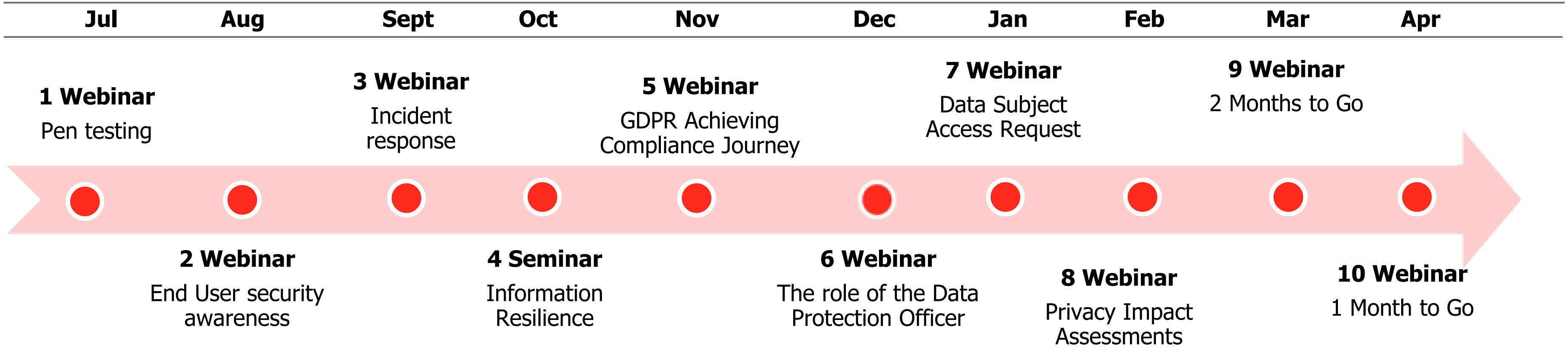
GDPR services, information lifecycle management and eDiscovery and forensics

Compliance and testing

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

bsi.

Path to GDPR – Cybersecurity and Information Resilience Services



Jul Aug Sept Oct Nov Dec Jan Feb Mar Apr

1 Webinar
Pen testing

2 Webinar
End User security awareness

3 Webinar
Incident response

4 Seminar
Information Resilience

5 Webinar
GDPR Achieving Compliance Journey

6 Webinar
The role of the Data Protection Officer

7 Webinar
Data Subject Access Request

8 Webinar
Privacy Impact Assessments

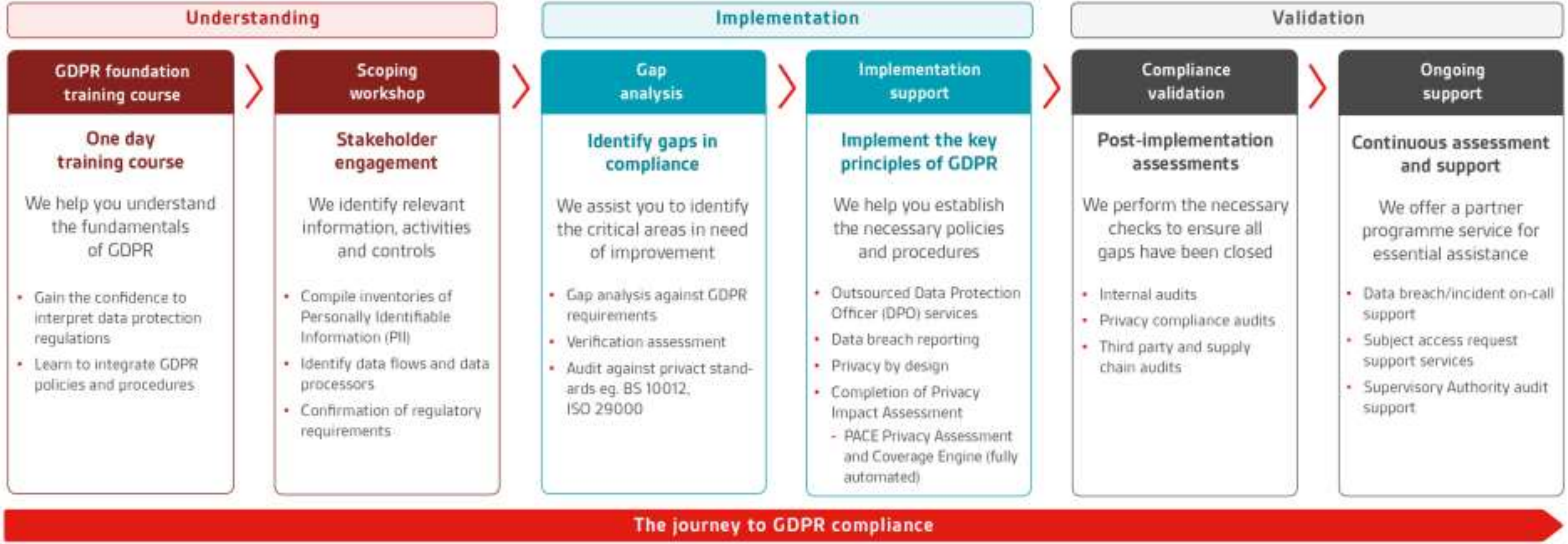
9 Webinar
2 Months to Go

10 Webinar
1 Month to Go

<u>Webinar Series:</u>

1. **Using penetration testing to keep your data safe** (Jul17)
2. **Untrained employees - the weakest link in your cybersecurity defence** (Aug17)
3. **You have 72 hours to respond after a breach… was personal data compromised?** (Sept17)
4. **Information Resilience Series Event** (Oct17)
5. **GDPR Achieving Compliance Journey** (Nov17)
6. **GDPR – the role of the Data Protection Officer** (Dec17)
7. **Getting ready to deal with Data Subject Access Requests (DSARs)** (Jan18)
8. **Privacy Impact Assessments (PIAs)** (Feb 18)
9. **2 months to go - the BSI achieving compliance guide - the first 10 of 20 steps analysed** (Mar 18)
10. **1 month to go - the BSI achieving compliance guide - the next 10 of the 20 steps analysed** (Apr18)

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 privact 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

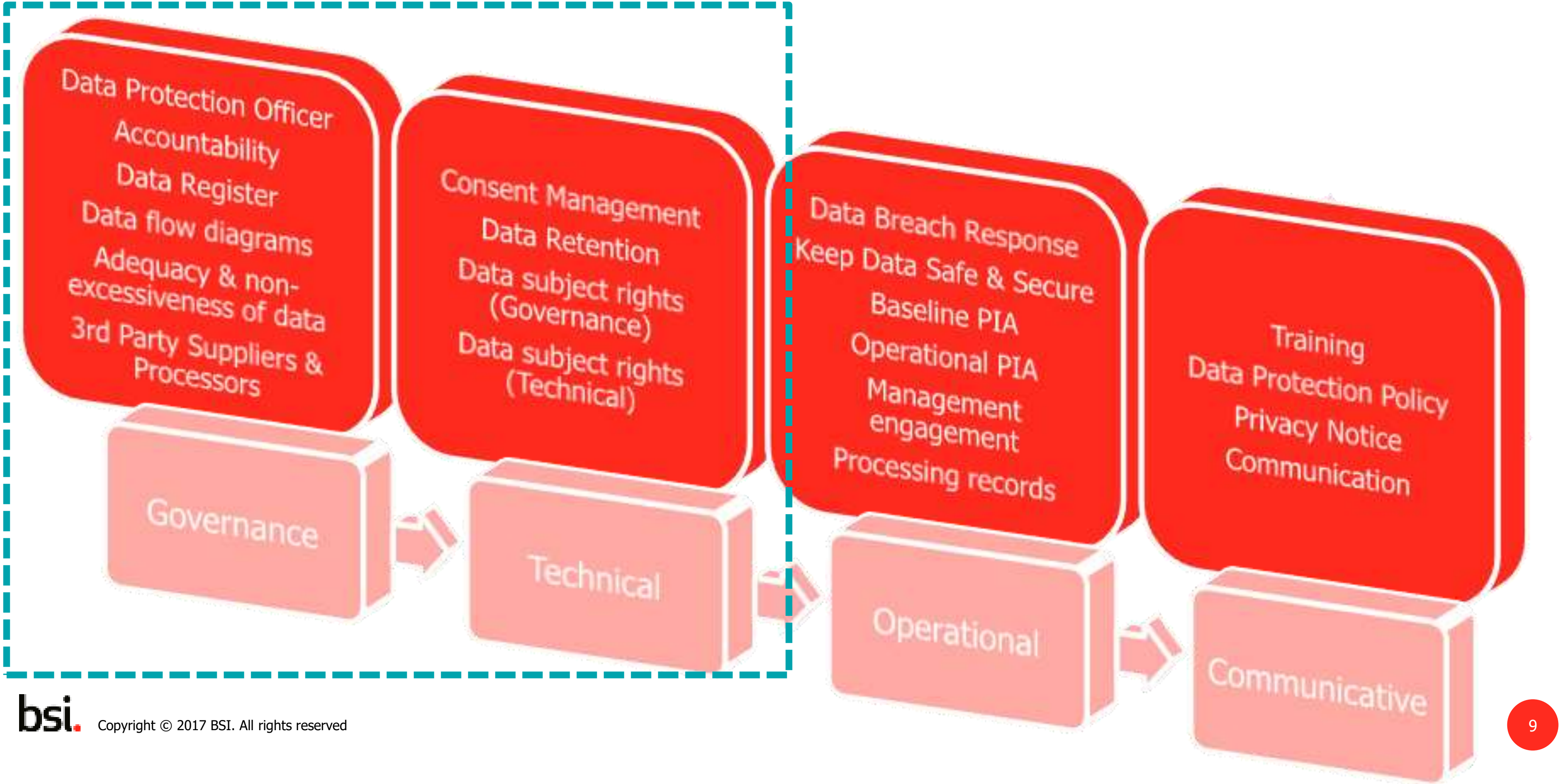
General Data Protection Regulation in 1 Minute

- 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



Data Protection Officer
Accountability
Data Register
Data flow diagrams
Adequacy & non-excessiveness of data
3rd Party Suppliers & Processors

Governance

Consent Management
Data Retention
Data subject rights (Governance)
Data subject rights (Technical)

Technical

Data Breach Response
Keep Data Safe & Secure
Baseline PIA
Operational PIA
Management engagement
Processing records

Operational

Training
Data Protection Policy
Privacy Notice
Communication

Communicative

The First 10 Steps

1. Assign a Data Protection Officer (DPO) – where necessary
2. Assign data ownership and accountability
3. Establish a Personal Data Register
4. Map out Data Flows
5. Ensure Adequacy and Non-Excessiveness of data
6. 3rd Party Suppliers & Processors
7. Ensure Proper Consent Management
8. Manage proper Data Retention
9. Data Subject Rights (Governance)
10. Data Subject Rights (Technical)

Step 1: Data Protection Officer

Governance

- Designate or outsource the DPO role;
- Ensure that DPO meets all training and competency requirements.
- Ensure that appointed DPO has no other operational conflicts of interest.

Difficulty level: Challenging

What is a DPO?

Under the GDPR

- A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR).
- Data Protection Officers are **responsible for overseeing** data protection strategy and implementation to ensure compliance with GDPR requirements

Qualifications

- The GDPR does not include a specific list of DPO credentials, but Article 37 does require a data protection officer to have "**expert knowledge of data protection law and practices**."
- The Regulation also specifies the DPO's expertise should align with the organization's data processing operations and the level of data protection required for the personal data processed by data controllers and data processors.

Do You Need a DPO?

- A DPO must be designated where:
  - The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
  - The organisations core activities involve "regular and systematic monitoring of data subjects on a large scale
  - The organisations core activities of the controller or the processor consist of processing on a large scale of special categories of data, and personal data relating to criminal convictions and offences

- **What's "LARGE SCALE"??**
- **What's Regular and Systematic Monitoring??**

- Also think about single DPO for a group (Article 37)
  - A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Tasks of the DPO (Article 39)

1. Inform and advise organisation and employees of obligations under GDPR
2. The DPO is the voice of data protection compliance within an organization
3. Monitor GDPR compliance for their organisation
4. Interface with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information
5. Training staff involved in safe data processing and data handling
6. Maintaining comprehensive records of all data processing activities conducted by the company

Tasks of the DPO (Article 39)

7. **Data Protection Impact Assessments (DPIAs)**
   - Monitoring performance
   - Providing advice on the impact of data protection efforts upon request [Article 35]

8. **Liaison with Supervisory Authorities**
   - Act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other relevant matter.
   - Cooperation with supervisory authority upon request (audit, complaint, information on processing activities
   - Data Breach reporting

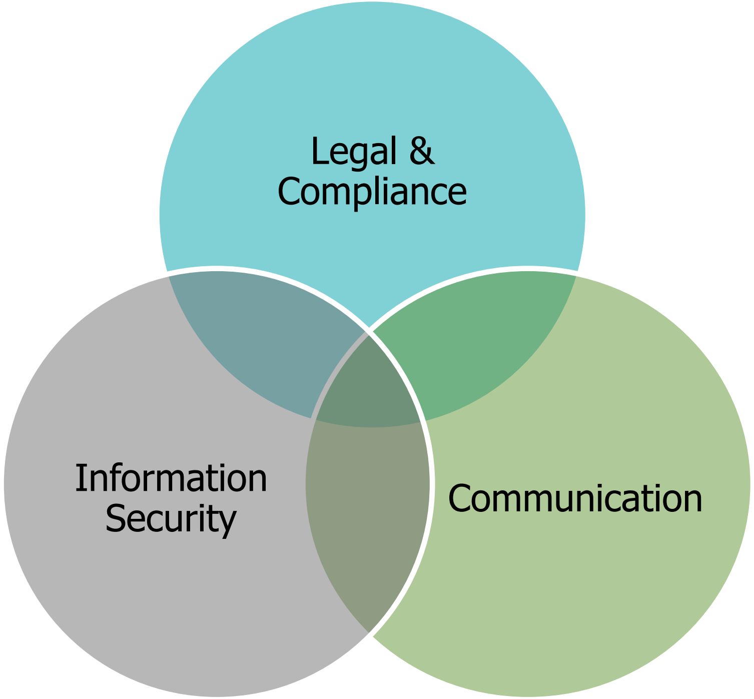
ico.
Information Commissioner's Office

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

bsi.

Expertise and Skills of a DPO (Article 37)

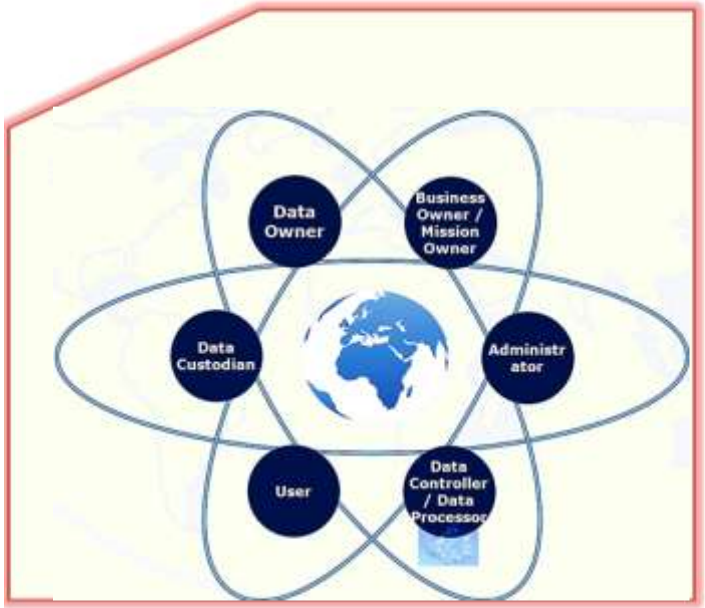
Overlap of Disciplines



Governance

Step 2: Accountability

- Assign data ownership responsibility to business unit heads/representatives.
- Most organisations will already understand this.

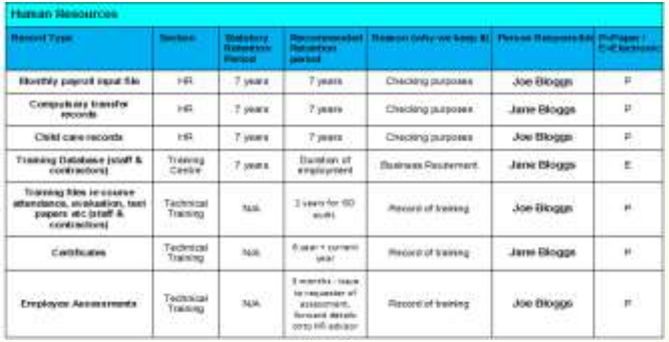

Data Owner
Business Owner / Mission Owner
Data Custodian
Administr ator
User
Data Controller / Data Processor

Difficulty level: Simple

Step 3: Personal Data Register

Governance

- You Can’t protect what you don’t understand
- Establishing a personal data register begins the process of understanding your data
- all personal data that the organization holds or processes should be recorded on that register
- Agree data register format and explain data owners’ obligation to complete the info register and set deadline.



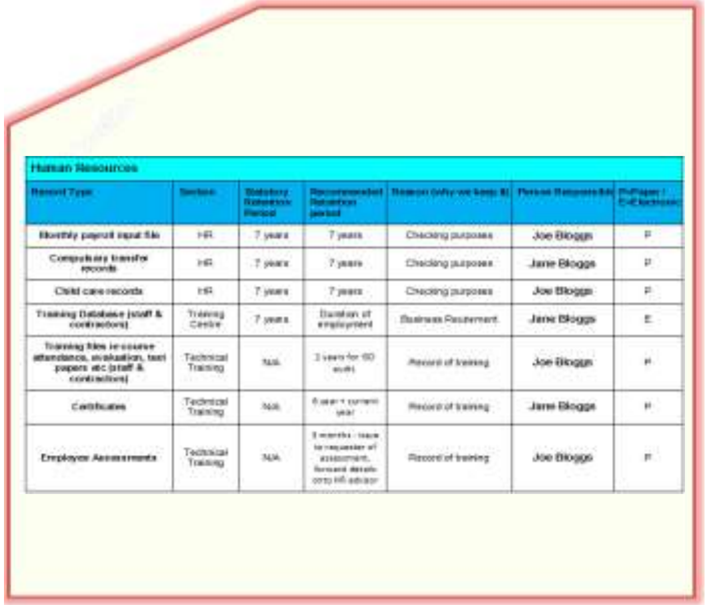
Human Resources						
Record Type	Section	Statutory Retention Period	Recommended Retention period	Reason (why we keep it)	Person Responsible	P=Paper / E=Electronic
Monthly payroll input file	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Compulsory transfer records	HR	7 years	7 years	Checking purposes	Jane Bloggs	P
Child care records	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Training Database (staff & contractors)	Training Centre	7 years	Duration of employment	Business Requirement	Jane Bloggs	E
Training files ie course attendance, evaluation, test papers etc (staff & contractors)	Technical Training	N/A	3 years for ISO audit	Record of training	Joe Bloggs	P
Certificates	Technical Training	N/A	6 years + current year	Record of training	Jane Bloggs	P
Employee Assessments	Technical Training	N/A	3 months - issue to requester of assessment, forward details onto HR advisor	Record of training	Joe Bloggs	P

Difficulty level: Simple

Step 3: Personal Data Register

Governance

- The Personal Data (or Information) Register should detail at least:
  - The names of filing systems which holds personal data
  - How the data is classified (personal vs special categories)
  - Approximate volumes/numbers of records
  - Purpose for processing the data
  - Legal basis for processing the data
  - How long is data retained for
  - Specific fields or types of data contained therein
  - The data owner.
  - Data format (paper vs electronic)
  - If any children's data held
  - Safeguards in place to protect data



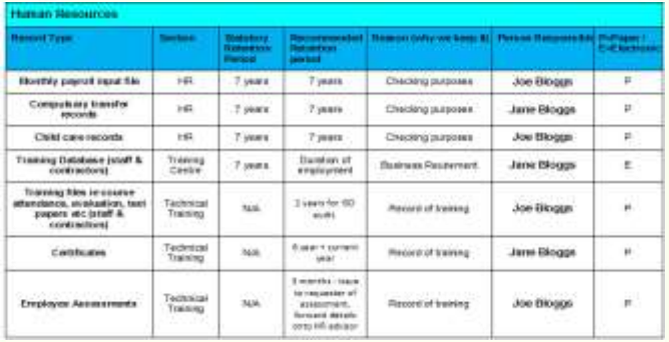
Human Resources

Record Type	Section	Statutory Retention Period	Recommended Retention period	Reason (why we keep it)	Person Responsible	P=Paper / E=Electronic
Monthly payroll input file	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Compulsory transfer records	HR	7 years	7 years	Checking purposes	Jane Bloggs	P
Child care records	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Training Database (staff & contractors)	Training Centre	7 years	Duration of employment	Business Requirement	Jane Bloggs	E
Training files ie course attendance, evaluation, test papers etc (staff & contractors)	Technical Training	N/A	3 years for ISO audit	Record of training	Joe Bloggs	P
Certificates	Technical Training	N/A	6 years + current year	Record of training	Jane Bloggs	P
Employee Assessments	Technical Training	N/A	3 months - issue to requester of assessment, forward details onto HR advisor	Record of training	Joe Bloggs	P

Difficulty level: Simple

Step 3: Personal Data Register

- Also Useful To Track:
  - Systematic sharing of personal data with 3rd parties
  - 3rd party requests for personal data (such as from legal authorities)
  - Details of any data flows involving transferring of personal data being sent outside of the EEA
  - tracking legal obligations to determine conflicts etc.
- For Data Processors:
  - What controller's we're working on behalf of
  - Types of processing and categories of data
  - Contacts details for data controllers
  - Data volumes
  - Authorisations



Human Resources

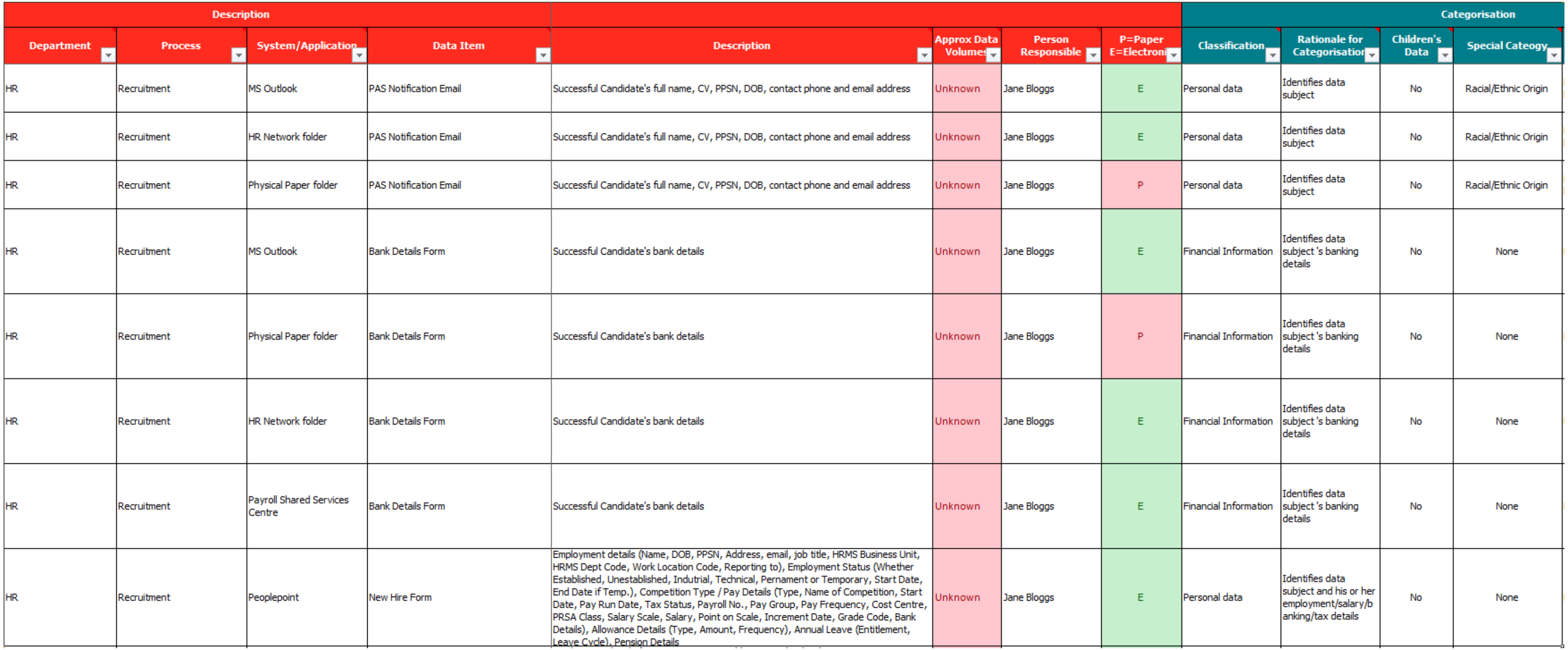
Record Type	Section	Statutory Retention Period	Recommended Retention period	Reason (why we keep it)	Person Responsible	P=Paper / E=Electronic
Monthly payroll input file	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Compulsory transfer records	HR	7 years	7 years	Checking purposes	Jane Bloggs	P
Child care records	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Training Database (staff & contractors)	Training Centre	7 years	Duration of employment	Business Requirement	Jane Bloggs	E
Training files ie course attendance, evaluation, test papers etc (staff & contractors)	Technical Training	N/A	3 years for ISO audit	Record of training	Joe Bloggs	P
Certificates	Technical Training	N/A	6 years + current year	Record of training	Jane Bloggs	P
Employee Assessments	Technical Training	N/A	3 months - issue to requester of assessment, forward details onto HR advisor	Record of training	Joe Bloggs	P

Difficulty level: Simple

bsi.

Step 3: Personal Data Register

Governance

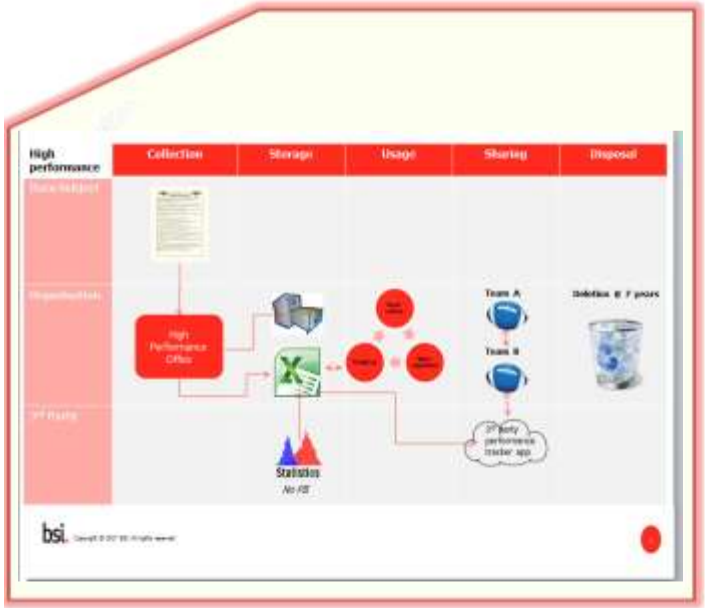


Description								Categorisation			
Department	Process	System/Application	Data Item	Description	Approx Data Volumes	Person Responsible	P=Paper E=Electroni	Classification	Rationale for Categorisatio	Children's Data	Special Cateogy
HR	Recruitment	MS Outlook	PAS Notification Email	Successful Candidate's full name, CV, PPSN, DOB, contact phone and email address	Unknown	Jane Bloggs	E	Personal data	Identifies data subject	No	Racial/Ethnic Origin
HR	Recruitment	HR Network folder	PAS Notification Email	Successful Candidate's full name, CV, PPSN, DOB, contact phone and email address	Unknown	Jane Bloggs	E	Personal data	Identifies data subject	No	Racial/Ethnic Origin
HR	Recruitment	Physical Paper folder	PAS Notification Email	Successful Candidate's full name, CV, PPSN, DOB, contact phone and email address	Unknown	Jane Bloggs	P	Personal data	Identifies data subject	No	Racial/Ethnic Origin
HR	Recruitment	MS Outlook	Bank Details Form	Successful Candidate's bank details	Unknown	Jane Bloggs	E	Financial Information	Identifies data subject 's banking details	No	None
HR	Recruitment	Physical Paper folder	Bank Details Form	Successful Candidate's bank details	Unknown	Jane Bloggs	P	Financial Information	Identifies data subject 's banking details	No	None
HR	Recruitment	HR Network folder	Bank Details Form	Successful Candidate's bank details	Unknown	Jane Bloggs	E	Financial Information	Identifies data subject 's banking details	No	None
HR	Recruitment	Payroll Shared Services Centre	Bank Details Form	Successful Candidate's bank details	Unknown	Jane Bloggs	E	Financial Information	Identifies data subject 's banking details	No	None
HR	Recruitment	Peoplepoint	New Hire Form	Employment details (Name, DOB, PPSN, Address, email, job title, HRMS Business Unit, HRMS Dept Code, Work Location Code, Reporting to), Employment Status (Whether Established, Unestablished, Indutrial, Technical, Permanent or Temporary, Start Date, End Date if Temp.), Competition Type / Pay Details (Type, Name of Competition, Start Date, Pay Run Date, Tax Status, Payroll No., Pay Group, Pay Frequency, Cost Centre, PRSA Class, Salary Scale, Salary, Point on Scale, Increment Date, Grade Code, Bank Details), Allowance Details (Type, Amount, Frequency), Annual Leave (Entitlement, Leave Cycle), Pension Details	Unknown	Jane Bloggs	E	Personal data	Identifies data subject and his or her employment/salary/banking/tax details	No	None

Step 4: Data Flow Diagrams

Governance

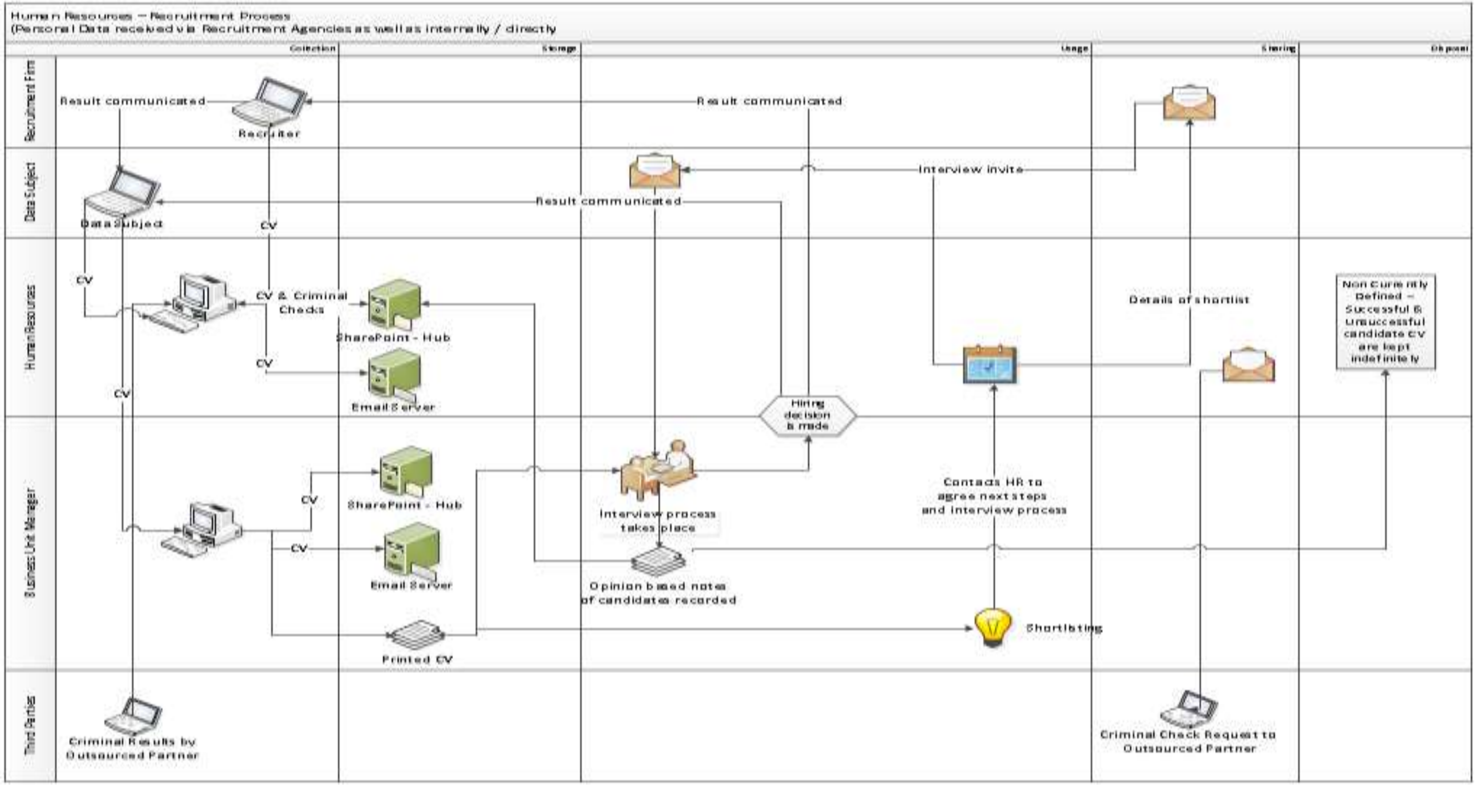
- To be done in conjunction with data owner:
  - Explain data owners’ obligation to help complete data flow diagrams
  - Initial meeting to discuss flows
  - GDPR lead to complete diagrams
- Diagrams should include:
  - Customer data details
  - Data volumes
  - Name of the system in which it is held
  - Business/technical owner
  - Details of 3rd parties to whom the data may be transferred (include security measures such as encryption)



Difficulty level: Low…”ish”

Step 4: Data Flow Diagrams

Governance



Human Resources – Recruitment Process
(Personal Data received via Recruitment Agencies as well as internally / directly

bsi.

Step 5: Adequacy & Non-excessiveness Of Data

Governance

- Once you understand what data you have, you can consider the adequacy of the information and the extent of the information that you have collected.

- **Data Minimisation:** The less data you maintain, then the smaller the effort involved in maintaining compliance on an ongoing basis.
  - Less data to keep safe and secure (including anonymising)
  - Less data to manage retention periods for
  - Less data to provide or delete when responding to Data Subject Access Requests (DSARs) and Right to Be Forgotten requests (more on these later)

Difficulty level: Medium

Step 6: 3rd Party Suppliers & Processors

Governance

- Where data is shared with 3rd parties, ensure appropriate security and privacy agreements are contractually agreed and enforced
- Ideally, contracts should include clauses to ensure that 3rd parties are processing data in a safe and secure manner and permit you to perform audits and spot checks to ensure compliance

Difficulty level: Challenging

Managing 3rd Parties

- Ensure that Data Protection requirements are mandated to all third parties with whom personal data might be shared (e.g. clients, vendors, processors/sub-processors, partners)

- Develop due diligence practices established to evaluate data protection and security posture of all potential contractors and vendors

- Conduct due diligence practices on all 3rd party data sources from whom personal data might be acquired

Step 7: Consent Management

Technical

Where consent is used **as basis for processing** data:

- Ensure that consent currently held will meet the requirements under the GDPR; if not, **re-obtain consent**.
- Ensure that all consents can be immediately demonstrated; if not, **re-obtain consent and maintain a consent record**.
- Where sensitive data (i.e. medical data / health data / claim data etc.), ensure that **additional explicit consent** has been obtained.
- Ensure process for **removal of consent is clearly communicated** at all points where data is collected and in privacy notice
- Identify any data relating to children; ensure consent from parent has been provided **and validated**; if not, re-obtain consent.

Difficulty level: Challenging

Step 8: Data Retention

Technical

- The reasons for processing and the length of time data should be retained will now be understood
- Begin enforcing retention period;
- Review your data registers and data flow diagrams and where any data has passed agreed retention deadlines you must now securely remove it.
- Delete any data that has passed agreed retention deadlines as per data register.
- Automate where possible!

Difficulty level: Low (But…)

Step 8: Data Retention – Challenges

Technical

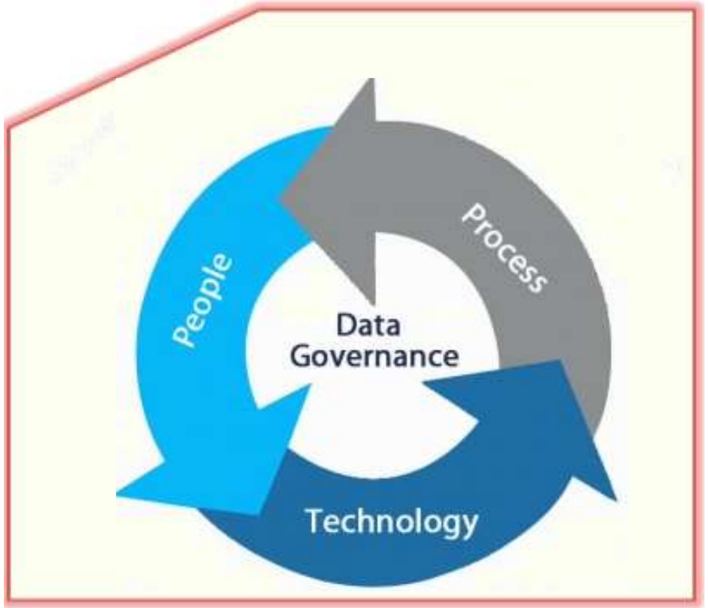
- Not all electronic systems allow for permanent deletion of records
  - Potential solution: encrypt / scramble the data to anonymise
- Conflicts between legal requirements to retain data vs Right to be Forgotten requests
  - D
- Enforcing retention/disposal of historical, physical records

Difficulty level: Low (But…)

Step 9: Data Subject Rights (Governance)

Technical

- A number of data subject rights have been clarified or introduced, which require both governance and technical approaches to build compliant response processes
- Agree and document **governance policy and processes** for responding to new requirements.
  - Subject access requests
  - Right to restriction of processing / objection
  - Right to rectify
  - Right to erasure
  - Right not to be subject to automated decision making / Right to not be profiled
  - Data portability

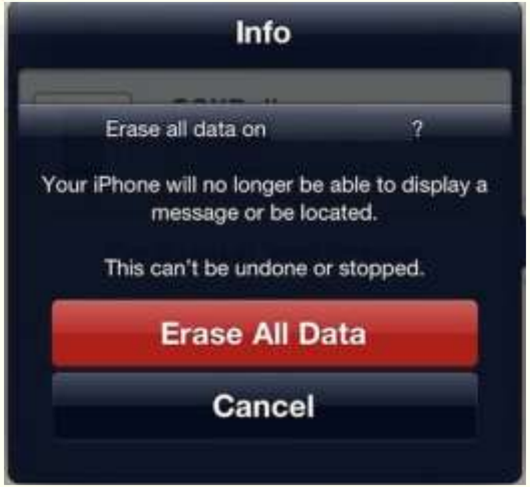


Difficulty level: Medium

Step 10: Data Subject Rights (Technical)

Technical

- Agree and document **your technical approach** to responding to new requirements.
  - Subject access requests
  - Right to restriction of processing / objection
  - Right to rectify
  - Right to erasure
  - Right not to be subject to automated decision making / Right to not be profiled
  - Data portability



Erase all data on ?

Your iPhone will no longer be able to display a message or be located.

This can't be undone or stopped.

Difficulty level: Challenging

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 can tailor solutions to businesses of all sizes and capabilities:

- Utilities
- Manufacturing
- Pensions
- Legal
- Technology
- Government
- Retail
- Transport

Get In Touch

Ireland

Phone: (+353) 1 290 1711

Email: cyber@bsigroup.com

Global

Phone: (+353) 1 210 1711

Email: cyber.ie@bsigroup.com