



GDPR readiness 20 steps to achieving compliance

Presented by:

Gavin D'Alton

Senior Data Protection & Privacy Consultant

BSI Cybersecurity and Information Resilience



**INVESTORS
IN PEOPLE**



**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

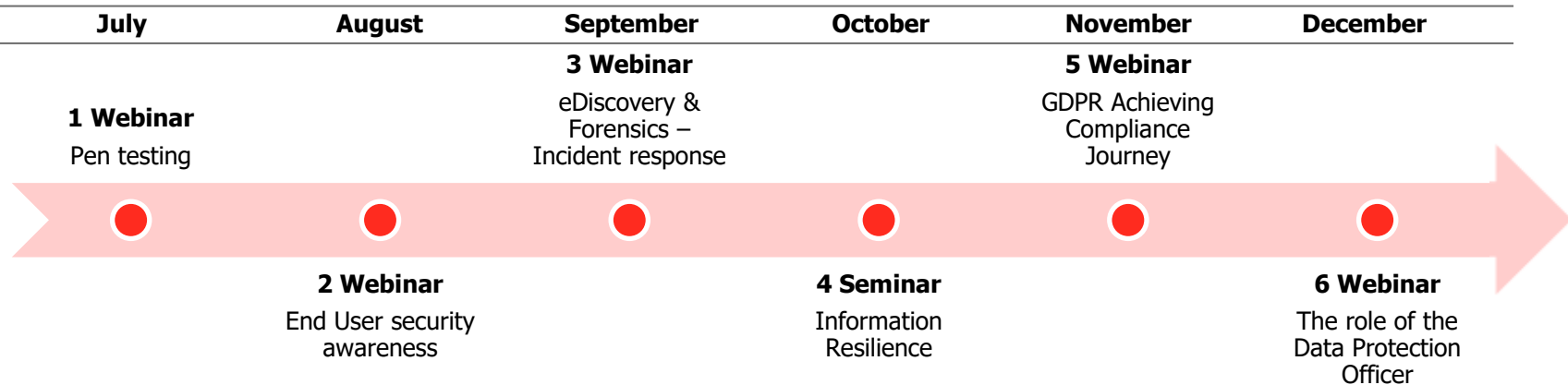


Compliance and testing

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?

Understanding

Awareness and training courses

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
- End user security awareness training

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 (e.g. BS10012, ISO 29000)

Implementation support

Implement the key principles of GDPR

We help you establish the necessary policies and procedures

- Outsourced Data Protection Officer services
- Data breach reporting
- Privacy by design
- Completion of Baseline Privacy Impact Assessment (PIA)
- Project/change based PIAs

Validation

Ongoing support

Validation and response services

We offer a partner programme service for essential assistance

- Audits - internal, 3rd party/ supply chain
- Data breach/incident on-call support
- Subject access request support services
- Supervisory authority audit support

Me!

ie.linkedin.com/pub/dir/Gavin/D'Alton

The screenshot shows a LinkedIn search results page. On the left, a profile card for Gavin D'Alton is visible, including his profile picture, name, and current role as Senior Manager at BSI Cyber Security & Information Resilience. On the right, a search filter sidebar is open, titled 'Find a different Gavin D'Alton'. This sidebar contains search input fields for 'First Name' and 'Last Name', an 'Example: Gavin D'Alton', and a list of search results. A red rounded rectangle highlights the search filter sidebar. The search results list includes three entries for 'Gavin Dalton' with different locations and one entry for 'Ann Swords' under the 'People Also Viewed' section.

Find a different Gavin D'Alton

First Name Last Name

Example: Gavin D'Alton

- Gavin Dalton**
V.P. of Finance & Business
Development at Resorts West
Greater Salt Lake City Area
- Gavin Dalton**
Greater New York City Area
- Gavin Dalton**
United States

[More professionals named Gavin D'Alton](#)

People Also Viewed

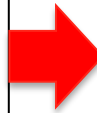
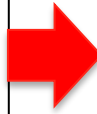
- Ann Swords**
Recruiter at Realex Payments
- Matej Saksida, CISM**
Experienced Certified Information
Security Manager | Application and
Infrastructure Security Team Lead |
PCI-DSS Expert

Lots of Noise...



Rules to Principals

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was given to you initially
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request



1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality

Rec.59; Art.12(2)

- Controllers have a **legal obligation to give effect to the rights of data subjects.**

General Definitions & Concepts

- **Data Subject:** User or Person
- **Data Controller:** Defines the data collected and reasons
- **Data Processor:** Processes data on behalf of the data controller
- **Supervisory Authority:** Data regulator

Timelines & Applicability for the GDPR

Timeline: Directive (EU) 2016/80 and Regulation (EU) 2016/679

- EU Data Protection Regulation **published** 2016
- The **Regulation** enters **into force** on 24 May 2016
- It shall **apply from** May 25th 2018
- Applicable to all industries, sectors, etc.



Is my Client Data considered “Personal Data”?

- Can a living individual be identified from the data,
- Does the data ‘relate to’ the identifiable living individual, whether in personal or family life, business or profession?
- Is the data ‘obviously about’ a particular individual?
- Is the data ‘linked to’ an individual so that it provides particular information about that individual?
- Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?
- Does the data have any biographical significance in relation to the individual?
- Does the data focus or concentrate on the individual as its central theme rather than on some other person, or some object, transaction or event?
- Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

Why now?

- When the 1995 law came about, the internet was in its infancy (Our Digital DNA is now everywhere we go)
- And every country has interpreted things a bit differently...



A large teal arc graphic that starts from the left edge of the slide and curves downwards towards the bottom right corner.

20 Steps to GDPR Compliance

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

Analysis



Current State

Key



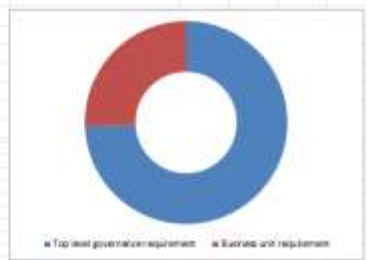
Desired State

Action Plan

Area	Section	Compliant	Non-Compliant	Partial	N/A	Total	Applicable	% Compliance
1	Maintain an Information Governance Programme	14	0	0	0	14	14	100
2	Maintain a Personal Data Inventory	5	1	2	0	7	7	71
3	Maintain Data Privacy Policy	5	0	3	0	5	5	100
4	Embed Data Privacy into Operations	15	3	0	0	27	27	56
5	Maintain a Training and Awareness programme	1	0	0	0	13	13	8
6	Manage Information Security Risk	13	0	0	0	13	12	100
7	Manage Third Party Risk	12	0	0	0	12	12	100
8	Maintain Privacy Notices	0	7	0	0	11	11	0
9	Respond to Requests and Complaints from Individuals	12	0	0	0	10	10	120
10	Monitor for New Operational Practices	12	0	0	0	7	7	171
11	Maintain Data Privacy Breach Management Program	7	0	1	0	8	8	88
12	Maintain Data Handling Practices	4	0	0	0	8	8	50
13	Track External Criteria	0	3	0	0	7	7	0

No. Questions	141
---------------	-----

Requirement	Total
Top level governance requirement	107
Business unit requirement	37
Governance & Business Unit	0



Requirement	Objective	Requirement Limit	Related Data Protection Principle	Related GDPR Article	Related Data Protection Principle	Related GDPR Article	Status	Recommendation
12 Monitor Data Handling Practices								
12.1	Does the organisation conduct regular self-assessments on privacy management?	Top level governance requirement		29	29		Partial	No Recommendation
12.2	Have internal audit assessments of the privacy program and privacy office been conducted?	Top level governance requirement					Partial	The organisation should conduct internal audit assessments of the privacy program and privacy office.
12.3	Are individuals responsible for data protection self-compliance conduct advised, made through self-assessments and data breach, facilities to evaluate practices adherence to data protection policies and procedures?	Top level governance requirement					Partial	No Recommendation
12.4	Are self-assessments of privacy management practices and procedures conducted in light of external events and data breaches?	Top level governance requirement					Partial	Self-assessments of privacy management practices and procedures should be conducted in light of external events and data breaches.
12.5	Has the organisation engaged with a 3rd party to conduct self-assessments of data protection management and procedures?	Top level governance requirement					Partial	No Recommendation
12.6	Are privacy management issues reported and reported to the executive board?	Top level governance requirement					Partial	The organisation should monitor and report privacy management issues to the executive board.
12.7	Is documentation regarding the privacy management established and maintained to demonstrate compliance and accountability?	Top level governance requirement		6	24		Partial	No Recommendation
12.8	Has the organisation sought to obtain and maintain certifications and accreditations to their data protection compliance for the supervisory authority?	Top level governance requirement					Partial	The organisation should seek to obtain and maintain certifications and accreditations to their data protection compliance for the supervisory authority.
13 Track External Criteria								
13.1	Does the organisation continuously monitor legal and regulatory requirements for data protection?	Top level governance requirement		26			Partial	The organisation should continuously monitor legal and regulatory requirements for data protection.
13.2	Has the organisation considered subscribing to compliance reporting services to gain insight into new developments regarding compliance requirements?	Top level governance requirement					Partial	The organisation should consider subscribing to compliance reporting services to gain insight into new developments regarding compliance requirements.
13.3	Does the organisation, where possible, attend and/or participate in privacy conferences and industry associations?	Top level governance requirement					Partial	The organisation should, where possible, attend and/or participate in privacy conferences and industry associations.

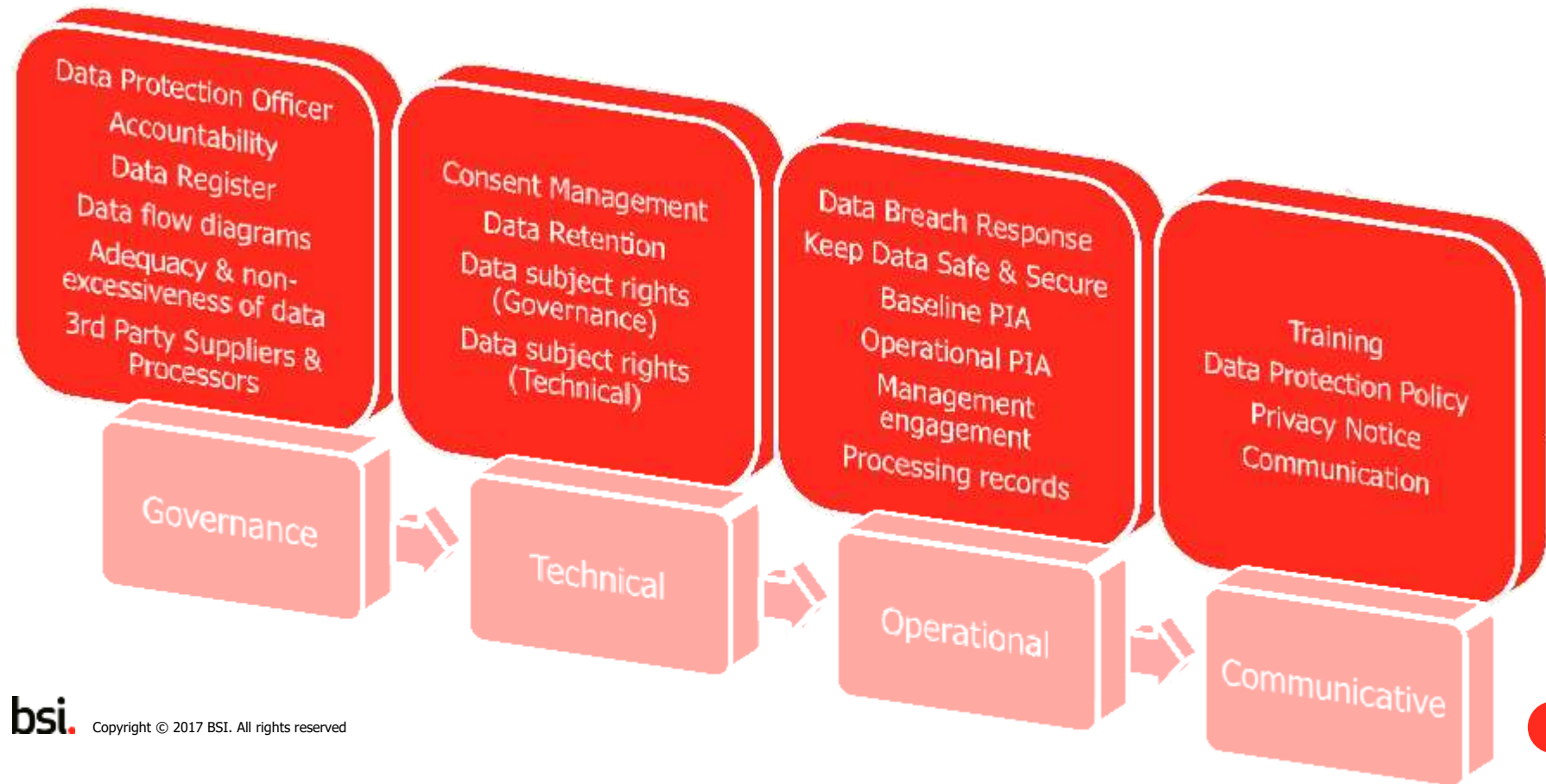


Actual Plan	Area	Ref	Action	Notes / Assignment Info	Status	Actions	Res. Skills
Data Protection (DS)	Data Protection (DS)	1.1	Organize an overview the DPO role	Ensure that appointed DPO has an other appropriate methods of interest / have the following roles are related and submit the appointed DPO due to appropriate methods: IT, Security, HR, Finance, Compliance (in the event that they process or handle PAs, etc.)	In progress	Self DPO or external firm appointed (Info, Security or HR)	ISA
		1.2	Ensure that DPO meets all training and competency	Supporter roles: DPO, CPM, CPO	Planned	Curriculum including ISO 27001, GDPR	ISA IS
	Data Register	2.1	Map: Data processing responsibility to business unit	Map: Data processing responsibility to business unit	In progress		ISA
		3.1	Complete Data register	The Information Register will need to detail: <ul style="list-style-type: none"> The names of systems which handle personal data How the data is processed Purpose for processing the data Legal basis for processing the data Who has or who retained but Special risks or types of data retention (where) The data owner 	In progress	Initial meeting held with Marketing and HR to bring Accounting into the Register Further meetings planned with: <ul style="list-style-type: none"> IT Operations Training/Compliance Marketing 	ISA IS
Data Register	Data Register	3.2	Implement data owners' obligation to complete the info register and set deadline	Completed during marketing meeting with IT/Security	In progress		ISA IS
		3.3	Identify the legal basis for processing of data	Legal basis = Legitimate interest, consent, legal mandate, etc.	Planned		ISA IS
		3.4	Ensure that retention period is clear	Marketing retention period is clear	Planned		ISA IS
		3.5	The mapping and review completed data registers will desktop owner or partner, better	Will be included in ongoing compliance projects	Completed		ISA IS
Data Register	Data Register	4.1	Complete data flow diagrams	To do: Data in conjunction with DPO owner <ul style="list-style-type: none"> Ensure data owner's' obligation to help complete data flow diagrams Initial meeting by DPO and HR GDPR lead to complete diagrams 	In progress	Initial meeting held with Marketing and HR to bring Accounting into the Register Further meetings planned with: <ul style="list-style-type: none"> IT Operations Training/Compliance 	ISA IS
		4.2	Organize an overview the DPO role	Ensure that appointed DPO has an other appropriate methods of interest / have the following roles are related and submit the appointed DPO due to appropriate methods: IT, Security, HR, Finance, Compliance (in the event that they process or handle PAs, etc.)	In progress	Self DPO or external firm appointed (Info, Security or HR)	ISA

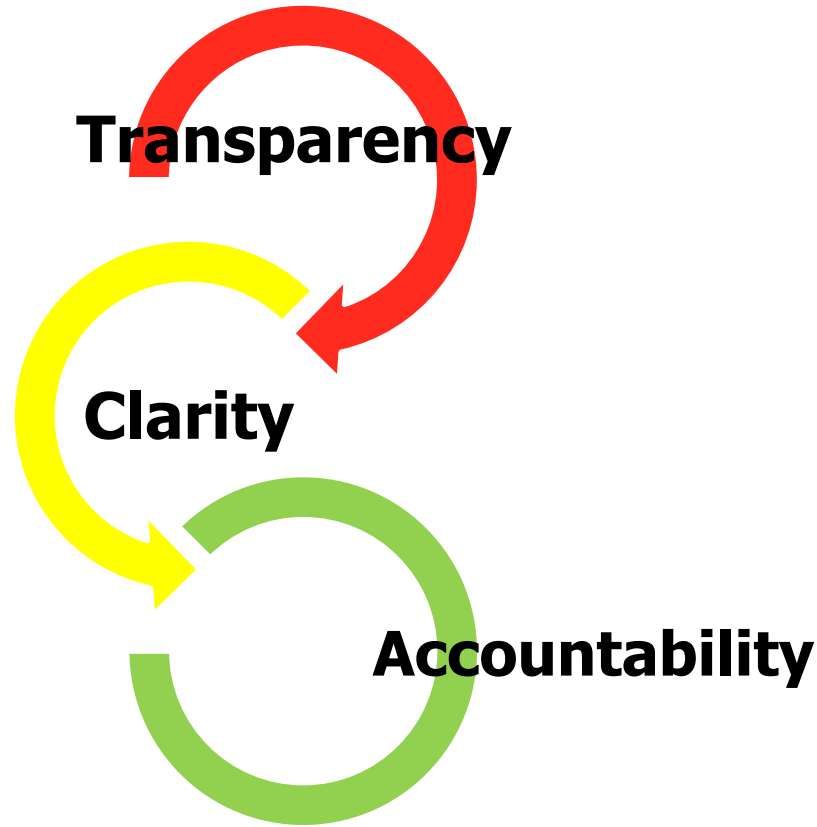
bsi.

Cybersecurity and Information Resilience

The aforementioned 20 steps...



Framework for our discussion



Step 1: Data Protection Officer



- 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.

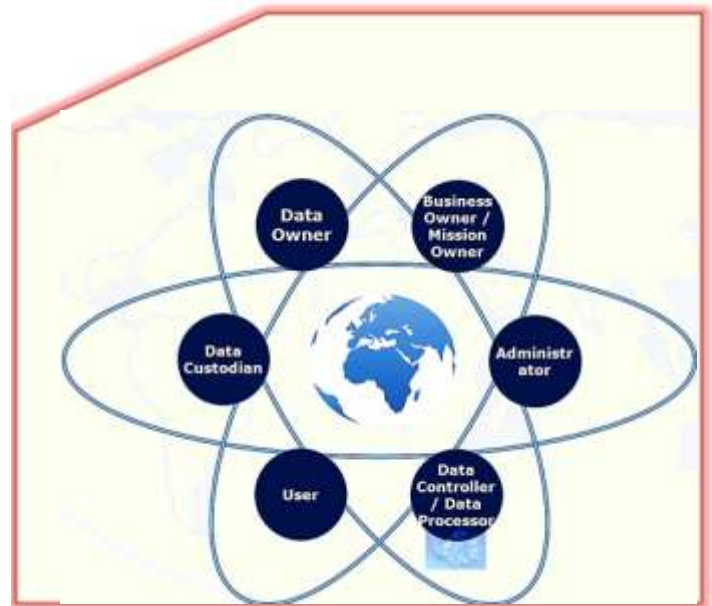


Difficulty level: Challenging

Step 2: Accountability



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



Difficulty level: Simple

Step 3: Data Register



- Agree data register format and explain data owners' obligation to complete the info register and set deadline.
- The Data (or Information) Register will need to detail at least:
 - The names of systems which holds personal data
 - How the data is classified
 - 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.

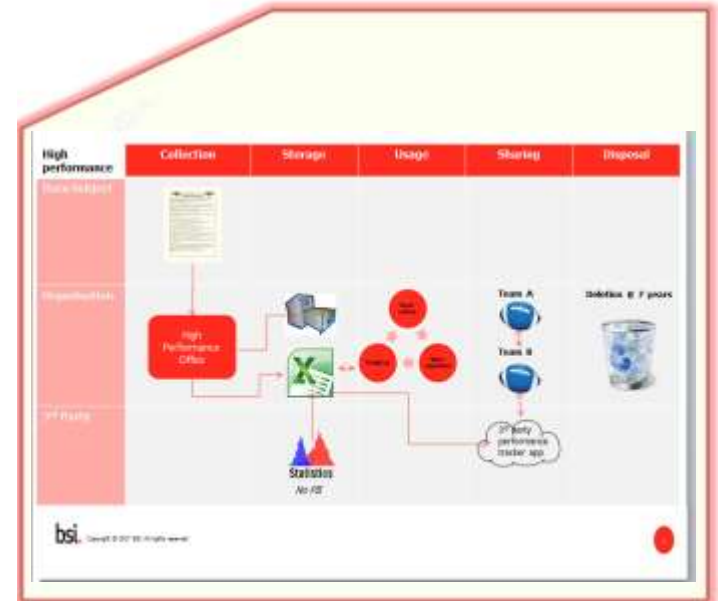
Human Resources						
Record Type	Section	Statutory Retention Period	Recommended Retention period	Source (why we keep it)	Person Responsible	P-Owner / EIC Addressed
Monthly payroll input file	HR	7 years	7 years	Checking purposes	Joe Bloggs	P
Compulsory transfer records	HR	7 years	7 years	Checking purposes	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 (e course attendance, evaluation, test papers etc (staff & contractors)	Technical Training	N/A	3 years for all staff	Record of training	Joe Bloggs	P
Certificate	Technical Training	N/A	8 year + current year	Record of training	Jane Bloggs	P
Employee Assessments	Technical Training	N/A	2 months - then in response of assessment, final answer will be added	Record of training	Joe Bloggs	P

Difficulty level: Simple

Step 4: Data flow diagrams



- 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 5: Adequacy & non-excessiveness of data



- On a “challenge basis”, review all data on information registers / data flows;
- If data is not absolutely required, delete and stop collecting it.
- This may require technical solutions!



Difficulty level: Medium

Step 6: 3rd Party Suppliers & Processors



- Where data is shared with 3rd parties ensure appropriate security and privacy agreements are contractually agreed and enforced.
- Perform audits and spot checks to ensure compliance.



Difficulty level: Challenging

Step 7: Consent Management



"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 under 18s; ensure consent from parent has been provided; if not, re-obtain consent.



Difficulty level: Challenging

Step 8: Data Retention



- Begin enforcing retention period;
- Delete any data that has passed agreed retention deadlines as per data register.
- Automate where possible!

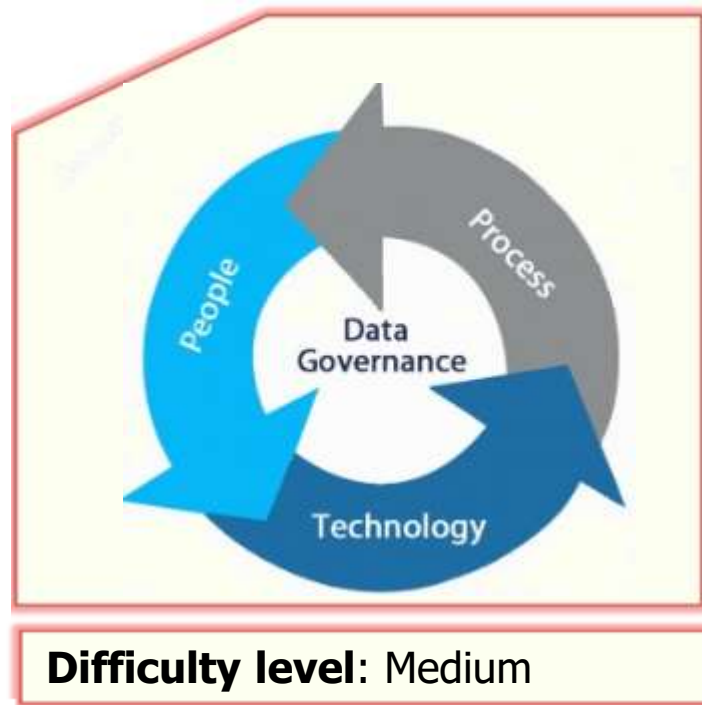


Difficulty level: Low (But...)

Step 9: Data subject rights (Governance)



- 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



Step 10: Data subject rights (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

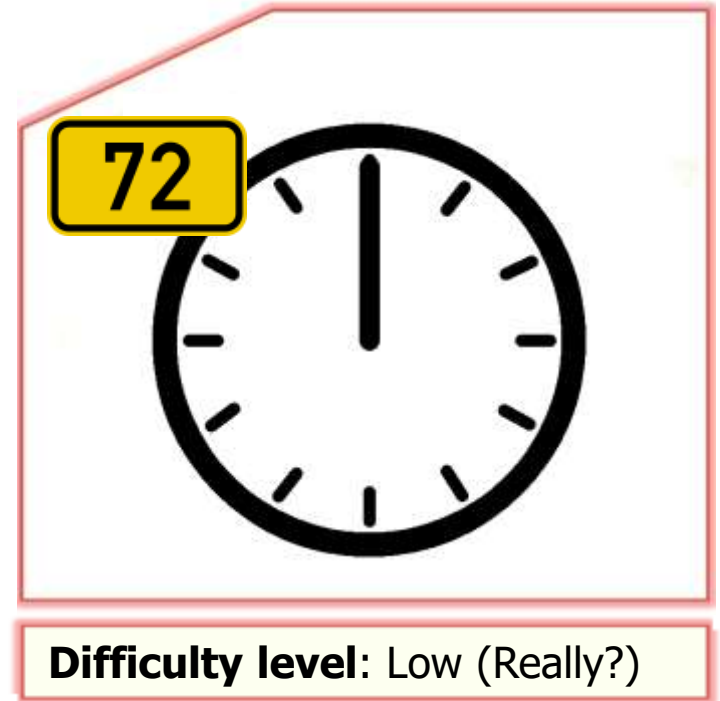


Difficulty level: Challenging

Step 11: Data Breach Response



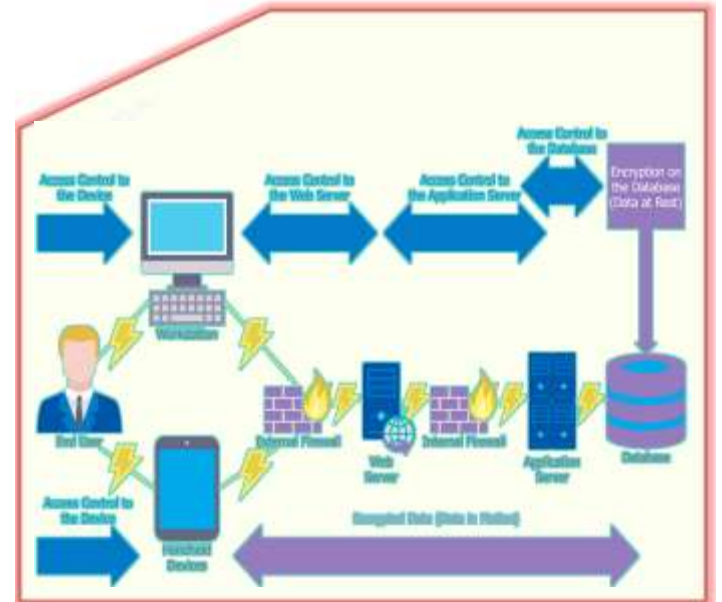
- Agree and document data breach / data security incident response process.
- Engage 3rd party expertise for
 - Forensic analysis
 - Incident response
 - PR / Communications to affected stakeholders



Step 12: Keep Data Safe & Secure

Operational

- Review security provisions in place for all data sets and data flows (i.e. control data at rest and data in transit)
- Rely on data registers and data flow diagrams (as discussed earlier)
- Risk prioritised approach!

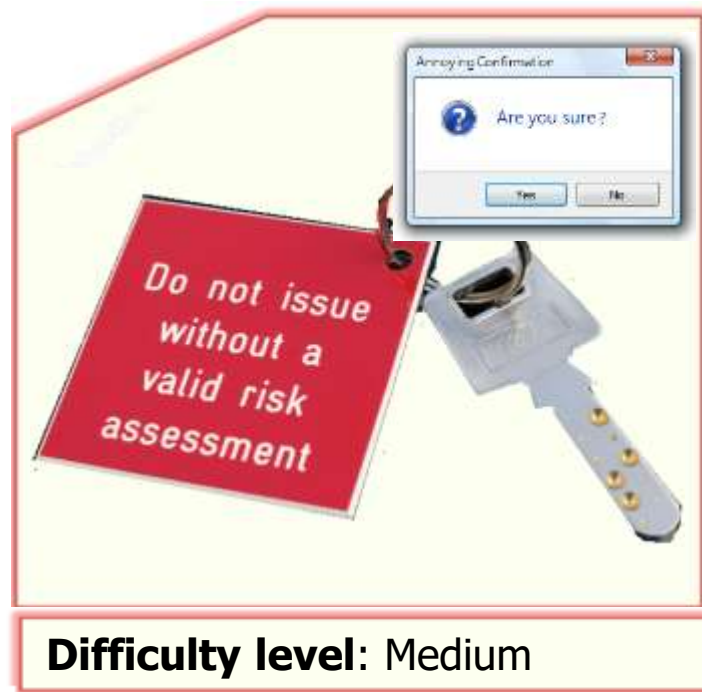


Difficulty level: Challenging

Step 13: Baseline PIA

Operational

- Privacy by design in practice.
- Complete baseline privacy impact assessment
- NOT a specific legal requirement under GDPR...
- BUT!



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.
- Action: Agree and present DP as a standing item at board meetings with relevant information / KPIs.
- Suggestion is that KPIs should include at least the following:
 - Incidents
 - Near misses
 - Access requests
 - Privacy risks to be monitored / Outputs from PIAs
 - Data shared with 3rd parties and plans to monitor compliance



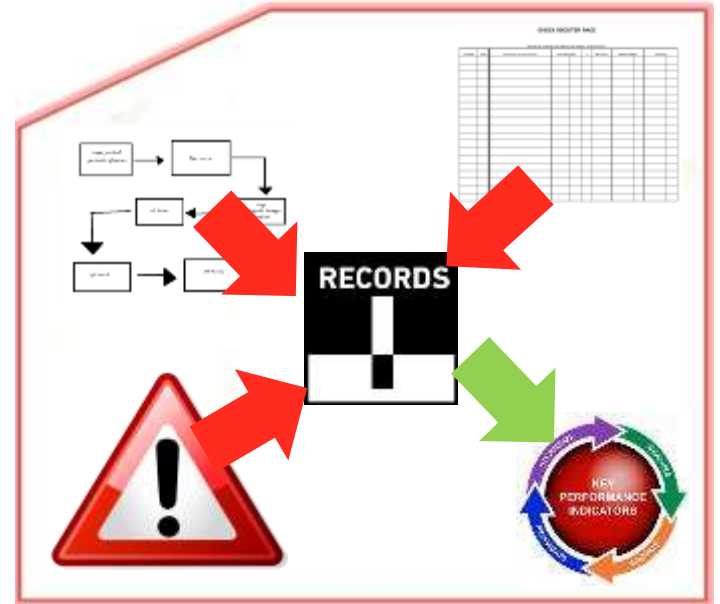
Difficulty level: Hmmmm...

Step 16: Processing records

Operational

- 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

Note: as per diagram...

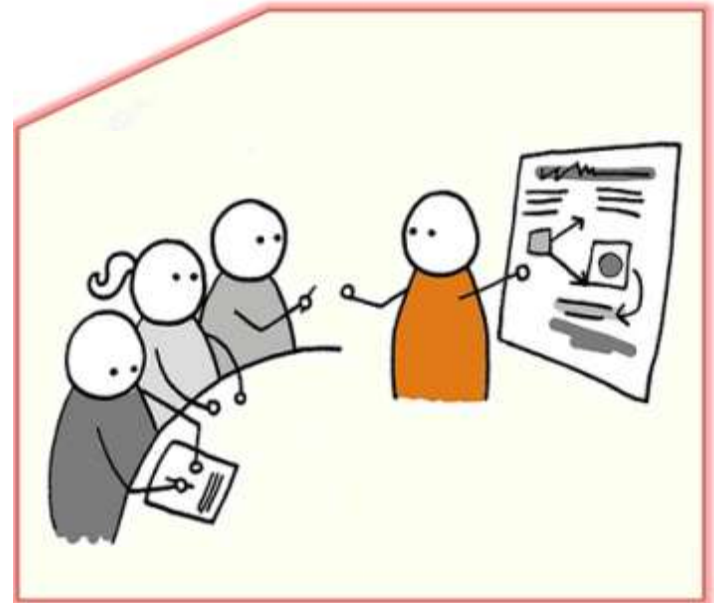


Difficulty level: Low (Really?)

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 18: Data Protection Policy



- Review and update **data protection policy** to account for outputs of all the above processes.

Document

Data Protection policy

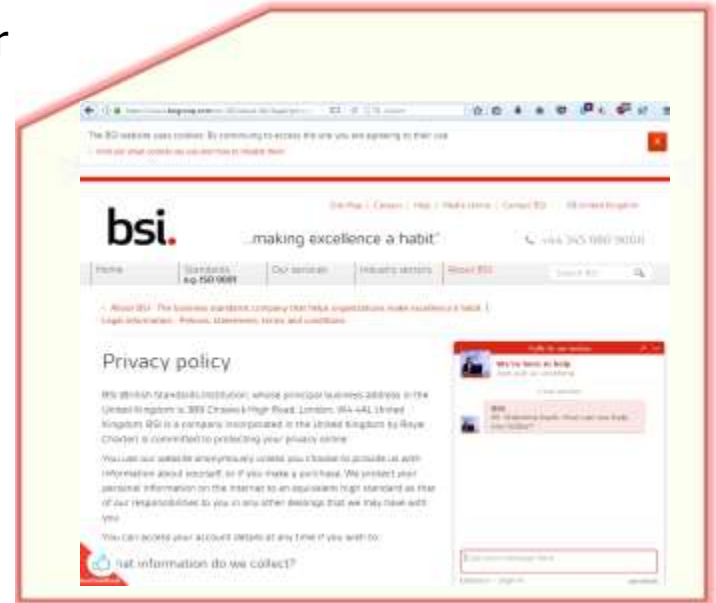
1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained 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



- Review and 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...)

A thick teal arc curves across the top and right side of the slide, framing the content.

Homework

Steps to follow in your own organisation

Your Plan for the next 7 months?

For more information

W: [bsigroup.com](https://www.bsigroup.com)

E: gavin.dalton@bsigroup.com

T: +353 (1) 210 1711

