

Dealing with Data Subject Access Requests

Sean Crowley - CIPP/E



INVESTORS
IN PEOPLE



By Royal Charter

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

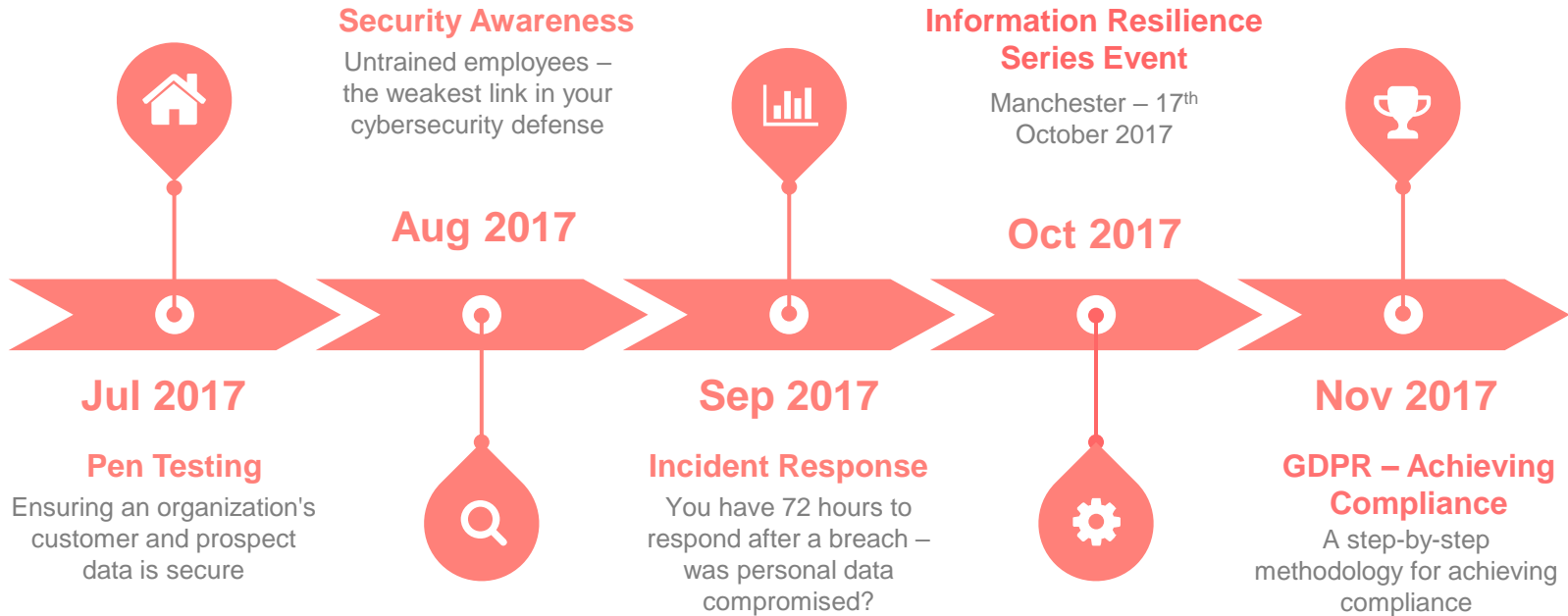
GDPR services, information lifecycle management and eDiscovery and forensics



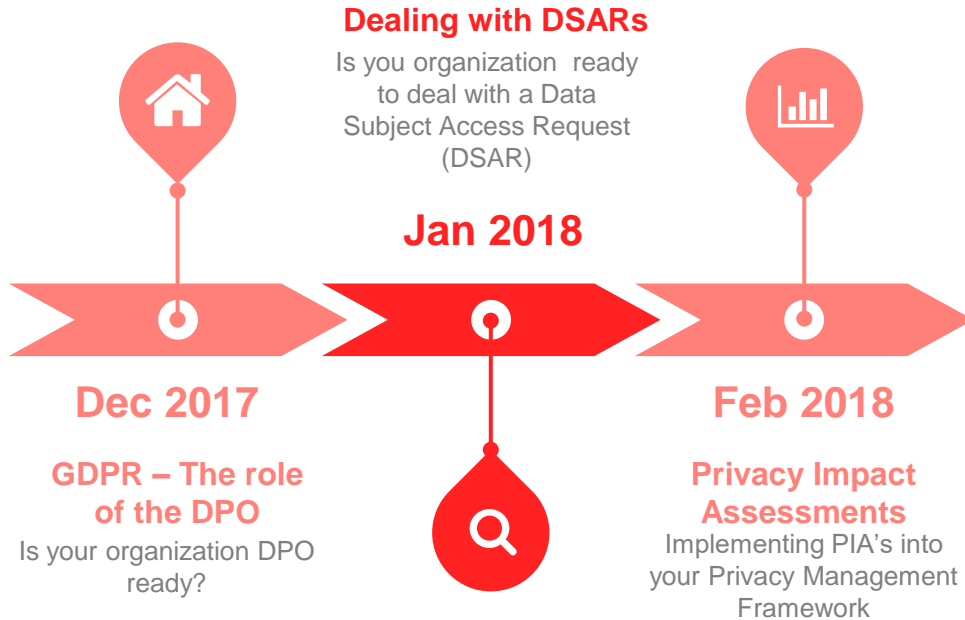
Compliance and testing

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

Path to GDPR – Cybersecurity and Information Resilience Services



Path to GDPR – Cybersecurity and Information Resilience Services



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

Agenda

This webinar will “hopefully” give you some insight into the following:

- What is the GDPR... in 1 minute
- What is a Data Subject Access Request... and why should you care
- What does a Data Subject Access Request look like
- Responding to a Data Subject Access Request
- Operationalizing the Data Subject Access Request Response
- Conclusion



What is the GDPR

...in 1 minute

What is the GDPR... in 1 minute

- The GDPR aims to **protect** the personal data of EU citizens
- It 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
- There is a requirement to **report** a data breach involving personal data to the supervisory authority within 72 hours of becoming aware of it
- **Fines** of up to €20m or 4% of annual worldwide turnover for non-compliance
- The regulation comes into force on the **25th May 2018**
- There will be a mandatory **Data Protection Officer** (DPO) requirement for some organisations
- No opt out for UK with **Brexit**



What is a Data Subject Access Request

... and why should you care

What is a Data Subject Access Request

Definition

- A Data Subject Access Request (DSAR) is the right of an individual to request any “personal data” that an organization holds on them.
- This right is a principle of the current EU Directive 95/46/EC and is retained in the GDPR.
- It is designed to regulate the processing of information from which a living individual can be identified or singled out either from the information on its own or when combined with other information.

What it means... For Individuals

The GDPR means a few things for Individuals when it comes for Access Rights under the new regulation, such as:

- There is more information out there for people regarding their rights
- Obtaining a copy of their personal information will be easier
- Obtaining a copy of their personal information will be faster



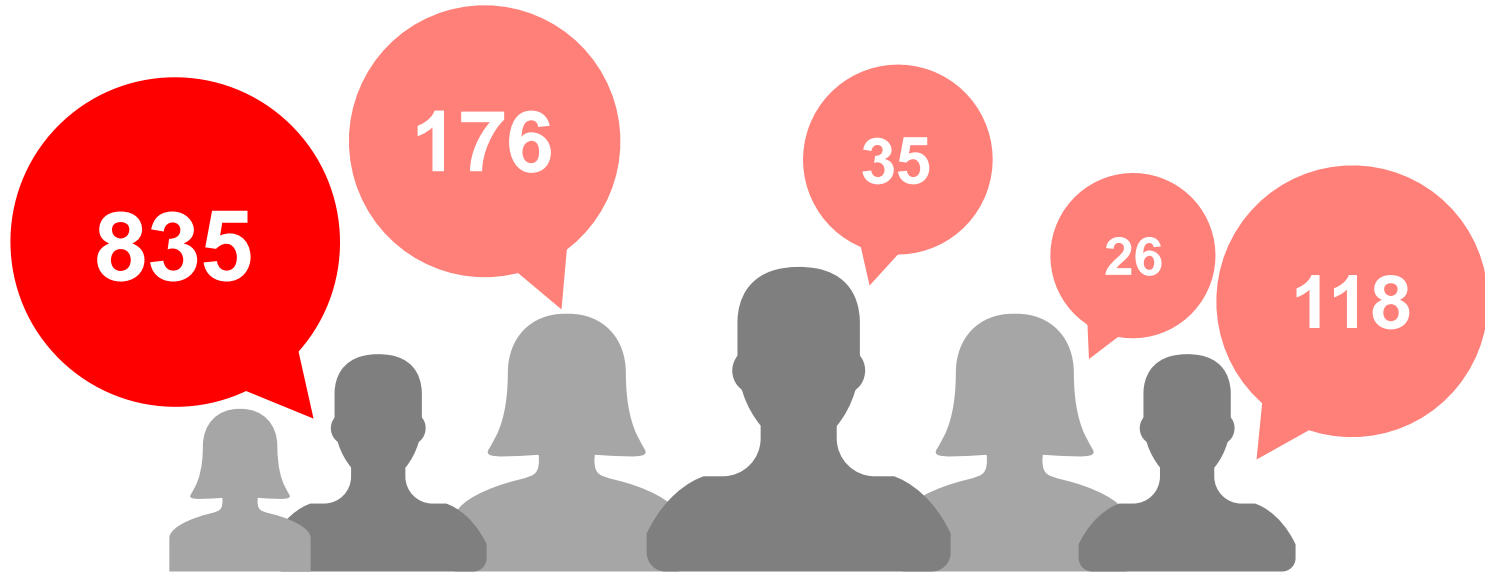
What it means... For Businesses

The GDPR also means a few things for Businesses when it comes for Access Rights under the new regulation, such as:

- No fees will be able to be charged to process Data Subject Access Requests
- Data minimization will no longer be a “nice to have” feature (if it ever was)
- Requests will need to be responded to within “one month”
- Process and procedures for dealing with Data Subject Access Requests will have to be developed



Some "Supervisory Authority" Statistics (2016)



Access Rights

The number of complaints received regarding Access Rights

Disclosure

The number of complaints received regarding unlawful disclosure

Security

The number of complaints received regarding the failure to secure data

Accuracy

The number of complaints received regarding the accuracy of data

Direct Marketing

The number of complaints received regarding electronic direct marketing

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

So, what does a Data Subject Access Request

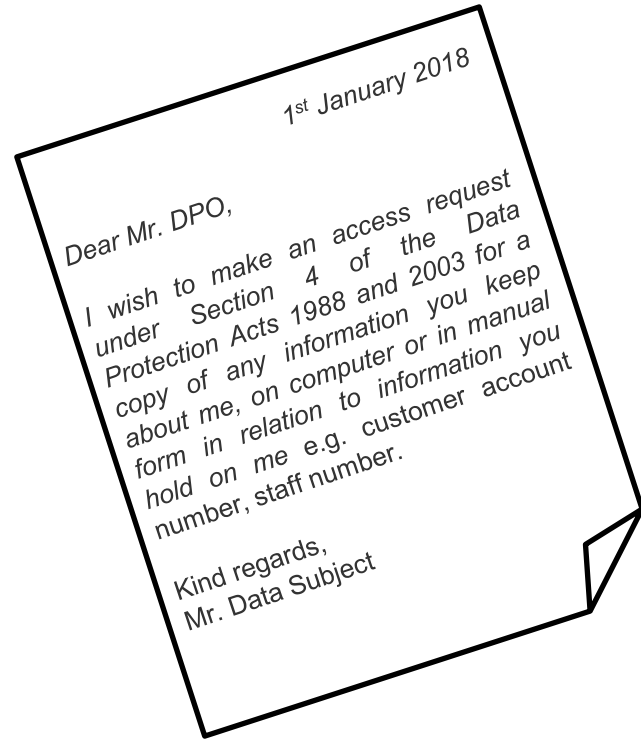
... look like

What does a Data Subject Access Request look like

We need to consider a couple of things here when discussing what a Data Subject Access Request looks like, namely:

- Who is submitting the request
- What is their motivation
- What is their level of knowledge of the regulation

Understanding these questions will determine if the request is **boilerplate** or **weaponized**



Lets talk about a Boilerplate Request

A typical Boilerplate Data Subject Access Request will generally consists of the following and look like this...

- A statement to stay that it is in fact a Data Subject Access Request
- Reference under what section of the specific Act it is referencing
- Details that may assist the organization find the individuals personal information

This is about as straight forward as the process is going to get



But wait... you mentioned a “Weaponized” Request



Sean Crowley

to [redacted]

12 Jan (10 days ago) ☆



Good afternoon [redacted]

Thanks from your email from [redacted] - Unfortunately, I wasn't expecting it.

Could you please provide the following as outlined below (which under European data protection laws I'm legally entitled to be provided with as a subject access request):

- Where, how and from whom you obtained my contact details?
- Where and how consent to send marketing information to my contact details was obtained?
- Details of all usages of my data (on a purpose by purpose basis – ideally, you might also please demonstrate what consent you obtained from me for each of those purposes).
- Any privacy notice employed at the point my data was collected.
- Can you please detail and provide a copy of the full data set relating to myself that you currently hold (including all email correspondence or CRM records where my name or this subject access request is mentioned). Please include (at least) the following:
 - Data in your database
 - Data in any backups of that database (on tape media, in mirrored databases, etc.)
 - Any physical / hard copies of my data
 - Any unstructured data (excel, word documents, etc.)
 - Where my data is stored and who can access it (particularly if it crosses any international borders)
 - How is the data secured (at rest and in transit)
 - Is the data encrypted (at rest and during transit)
 - How long will the data be retained for
 - How will all traces of the data be securely destroyed (including data in backups of databases, shares, email, etc.)

Can I also please have a copy of your data protection policy?

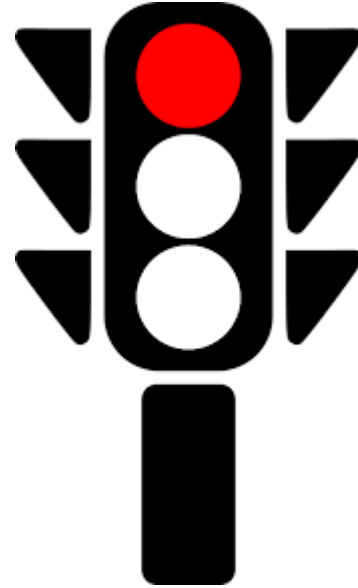
Please note, this subject access request has been submitted to you on 12/01/2018 – As it is required by the law, it would be great to have a response within 40 days (21/02/2018).

Sincerely,
Sean Crowley

Hang on, **STOP**. I can surely charge something for that

As mentioned on an earlier slide

- Come 25th May 2018 an organisation must provide a copy of the relevant information to a data subject free of charge
- ... Unless the organisation can prove that the request is manifestly unfounded or excessive
 - Proving this is often much easier said than done in reality



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

How do you respond to a Data Subject Access Request

Practical guidance

Rule 1: Be Polite



Rule 2: Identify the Individual

Remember...

- You don't have to supply any information until you have identified the individual
- This can include obtaining reasonable assurance that they are who they claim to be:
 - Passports
 - Drivers Licence
- This is to protect the "rights and freedoms" of the individual



Rule 3: Are you charging a fee

Remember...

- There is still scope to charge a nominal fee in some countries under the current Directive, for example:
 - £10 in the UK
 - €6.35 in the Republic of Ireland
- This **deterrent** will be **removed** in the new regulation



Rule 5: Is the Information Dynamic

Remember...

- You can still make routine changes to the data after getting the request
- That means amendments and deletions

However...

- Such changes should only be part of routine business practices
- It's not an excuse to remove embarrassing information (if you wouldn't write it on a postcard, don't write it in an email)



Rule 6: Other people have the right to privacy too

Remember...

- You do not have to give out information belonging to other Individuals as part of the request

However...

- This does not mean that you can blanketly refuse to release all information
 - Redaction is one option
 - Consent from the other Individuals is another option



Rule 7: Do any exemptions apply

Remember...

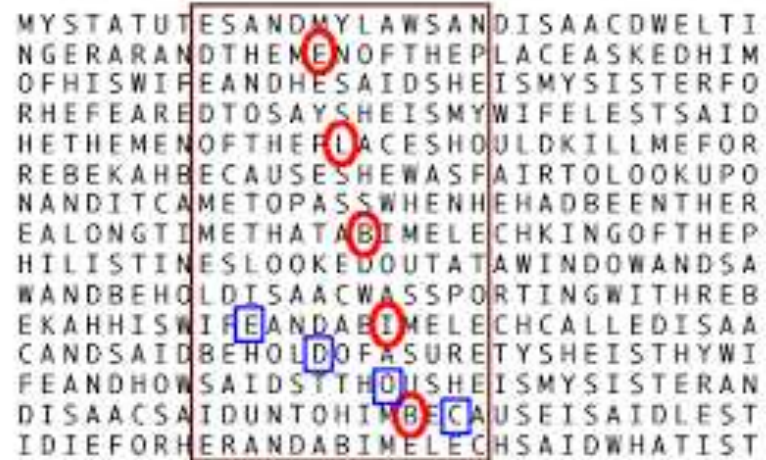
- You do not have to give out information if it falls under an exemption.
- Examples may include, but are not limited to:
 - Confidential references
 - Publicly available information
 - Intellectual property
 - Legal advice
 - Crime and taxation
 - Health records



Rule 8: Are any complex codes used

Remember...

- If complex codes are used that can identify the individual, these must be produced and explained as part of the response
- This could be a symbol that is used in a database where the only means of identification is using a key held by the organisation



MYSTATUT ESANDMYLAWSANDISAACDWELTI
NGERARANDTHEMENOFTHEPLACEASKEDHIM
OFHISWIFEANDHESAIDSHHEISMYSISTERFO
RHEFEAREDTOSAYSHEISMYWIFELESTSAID
HETHEMENOFTHEPLACESHOULDKILLMEFOR
REBEKAHBECAUSE SHEWASFAIRTOLOOKUPO
NANDITCAMETOPASSWHENHEHADBEENTHER
EALONGTIMETHATABIMELECHKINGOFTHEP
HILISTINESLOOKEDOUTATAWINDOWANDSA
WANDBEHOLDTISAACWASSPORTINGWITHREB
EKAAHISWIFEANDABIMELECHCALLEDISAA
CANDSAIDBEHOLDOFASURETYSHEISTHYWI
FEANDHOWSAIDSTHOUISHEISMYSISTERAN
DISAACSAIDUNTOHIMBECAUSEISAIDLEST
IDIEFORHERANDABIMELECHSAIDWHATIST

Rule 9: Prepare the Response

Remember...

- You only have **one month** from the time you have identified the individual
- This is a short period of time if you are not prepared
- **Tick tock**



What happens if I don't respond

Remember...

- Hiding from the issue is never an appropriate way to deal with a Data Subject Access Request
- If the Individual makes a complaint to the Supervisory Authority, they will likely issue you with a letter of investigation
- A formal investigation could land your organization with a fine

A large teal arc graphic that starts from the left edge of the slide and curves downwards and to the right, framing the main title.

Operationalizing the Data Subject Access Request Response

What BSI recommend

A Structured Approach is needed

BSI recommend a structured approach using the following steps:

- You **Recognize**
- You **Review**
- You **Verify**
- You **Acknowledge** or **Refuse**
- You **Engage** with the Individual
- You **Plan, Find** and **Retrieve**
- You **Produce** the information
- You **Document** your activities
- You **Balance** the rights of others vs the individual



Recognize

Ask yourself these questions

- What does a subject access request:
 - Look like?
 - Sound like?
- Are staff trained to recognise a subject access request?
- When a subject access request has been recognised, what process should staff enact?
 - Who does it get directed to?
 - When does it need to be forwarded on?



Review

Ask yourselves these questions

- Is it a Data Subject Access Request?
- Is it a valid Data Subject Access Request?
- Consider:
 - The source of the request
 - The information requested (is it PII or otherwise)
 - Is it manifestly excessive?



Verify

- You cannot assume that, on every occasion, the person making a request is who they say they are
- It is reasonable to require verification before sending information
- Should be considered on a risk prioritised basis:
 - An internal HR data request would not require this
 - A request only received via email would necessitate this



Acknowledge or Refuse

- Acknowledge the request as soon as possible
 - Its good practice to be clear on the date that the subject access request will be provided
 - Manage requesters expectations
 - If an extension would be required (90 days, in limited circumstances), this would be negotiated now
- If refusing the request, the onus is on the organisation to provide a robust justification as to why the request will not be fulfilled
- In the event that a request is rejected by an organisation, the requester has the right to escalate to their supervisory authority for mediation

Engage with the Individual

Early engagement can be crucial...

- Attempt to narrow the focus
- You cannot force the requester to narrow the scope of their request, but merely to provide additional details that will help you locate the requested information
- Similarly - Clarifying the request
 - Before responding to a SAR, you may ask the requester for information you reasonably need to find the personal data covered by the request
 - You need not comply with the SAR until you have received it
 - However, even if the relevant information is difficult to find and retrieve, it is not acceptable for you to delay responding to a SAR unless you reasonably require more information to help you find the data in question

Plan, Find and Retrieve

It is not always a straight forward process...

- Project plan may be required
- Organisation must be satisfied that they have identified all potential data sources / sets before proceeding
- Ideally, this can be based on pre-existing information registers, flows and data classifications
- In practice, a discovery process will be required
- All data should be collated into a central repository, to allow for formal production

Produce and Deliver

Leave production and delivery time...

- All data identified during discovery and based on requesters will have to be formally compiled
- Data must be presented in understandable format
- Data may be produced as physical/hard copy, or as soft copy; this should be agreed with the requester
- Personal data should be highlighted
- Supply and transfer in a secure manner or could be considered a breach

Document activities as you go

Document your decisions...

- Organisations are advised to document all activities and maintain records:
 - Decisions made
 - Data discovery methods / processes / timeframes / etc.
- Rationale: Even after data has been produced, organisations can expect data subjects to challenge the approaches taken
- Unless process can be robustly defended, the requester has scope to make a complaint to supervisory authorities

Considering the “rights and freedoms” of others

Rule:

- The GDPR says you do not have to comply with a DSAR if to do so would mean disclosing information about another individual who can be identified from that information.

Rule in practice:

- You should make decisions about disclosing third-party information on a case-by-case basis
- You must not apply a blanket policy of withholding it
- Best practice approach – either:
 - Get consent from other data subjects, or
 - Redact

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

Conclusion

How can BSI help

The Good News

BSI Cybersecurity and Information Resilience consultants provide:

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



Where we have worked

BSI can tailor solutions to businesses of all sizes and capabilities:

- Utilities
- Credit Unions
- Pensions
- Legal
- Technology
- Government
- Retail
- Transport

Get in touch

UK

Phone: 00 44 345 222 1711

Email: cyber@bsigroup.com

Global

Phone: 00 353 1 210 1711

Email: cyber.ie@bsigroup.com