

bsi.

Privacy Impact Assessments and Privacy By Design – What you need to know

Seamus Galvin

Senior Research and Development Consultant
BSI Cybersecurity and Information Resilience



**INVESTORS
IN PEOPLE**



By Royal Charter




Introduction.....



Seamus Galvin

Innovation and Research Manager

BSI • University of Limerick

Ireland • 323 

bsi.

Dublin, Ireland

- Market Analysis
- Commercial Assessment
- Innovation Support
- Technology R&D

seamus.galvin@bsigroup.com



BSI 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.



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 GDPR Compliance Professional Services

Understanding

Implementation

Validation

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

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)

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

Path to GDPR – Cybersecurity and Information Resilience Services

July

August

1 Webinar
Pen testing



2 Webinar
End User security awareness

Webinar Series:

1. Penetration Test
2. End User Security
3. Incident Response
4. Information Resilience
5. GDPR Achieving
6. GDPR – the role of
7. Getting Ready to

#8 - Privacy Impact Assessments (PIAs)

Date: Thursday 22 February
Time: 10:00 UK Time

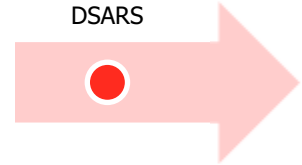


[More Info & Registration](#)

What is a PIA?
When are they required under GDPR?
And how do you integrate them into planned (or existing) project activities as part of privacy-by-design and overall privacy management?

January

7 Webinar
Managing DSARS



Secure
cybersecurity defence
data compromised?

ing compliance
ready?
ly to respond

Webinar Objectives

1. What is a Privacy Impact Assessment (PIA?)
2. PIA Requirements under GDPR
3. PIAs in relation to privacy-by-design and GDPR compliance
4. How do I know when a PIA is necessary?
5. Key stages to consider when completing a PIA
6. Tips for integrating PIAs into project and program management
7. Intro to BSI PACE (Privacy Assessment Coverage Engine) – using it to support PIAs and other privacy assessments



What's a PIA (or DPIA)?

At its core, a PIA is a **risk-based** assessment to ensure **rights and freedoms of data subjects** are protected when any processing about them is performed

Article 90 GDPR/ISO 31000

1. Establish context of proposed processing
2. Assess those risks
3. Treat/minimise those privacy risks

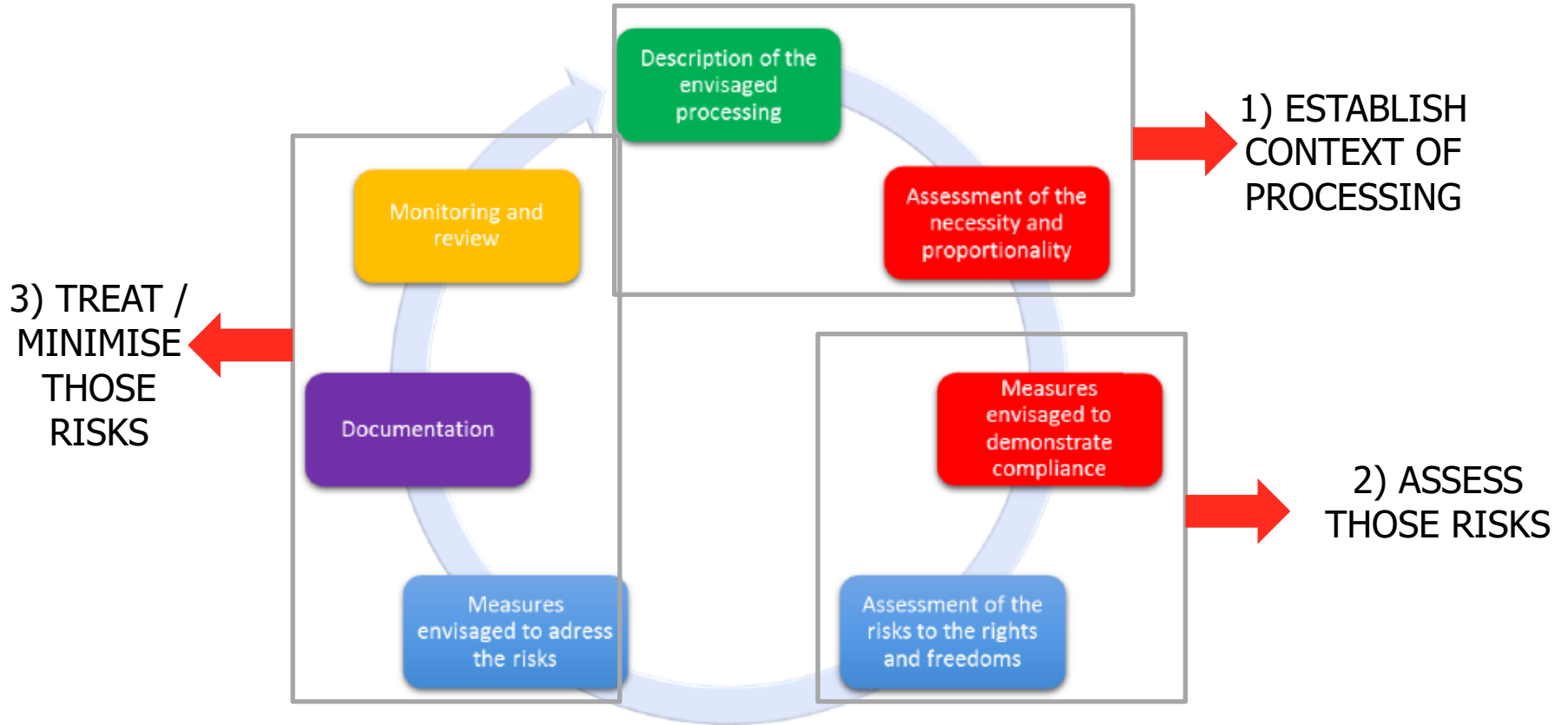
PIAs are a key tenet of Privacy-by-design
(the earlier the better!)



Data protection
impact
assessment (DPIA)



What's a PIA (or DPIA)?



Why Privacy-By-Design (and PIAs) ??

1. Key weapon in ensuring implementation of privacy at **tactical/operations levels**
2. Essential tool in **minimising (privacy + security) risk**
3. Builds **trust + transparency** with data subjects and stakeholders
4. Supports **identifying problems early** in projects (when they are cheaper to fix)
5. Key to **increasing awareness** of privacy across the organisation
6. Increases likelihood of **compliance with GDPR** and other privacy regulations
7. Actions are **less likely to be privacy intrusive** – and have negative impact on individuals.



Are PIAs just about GDPR compliance?

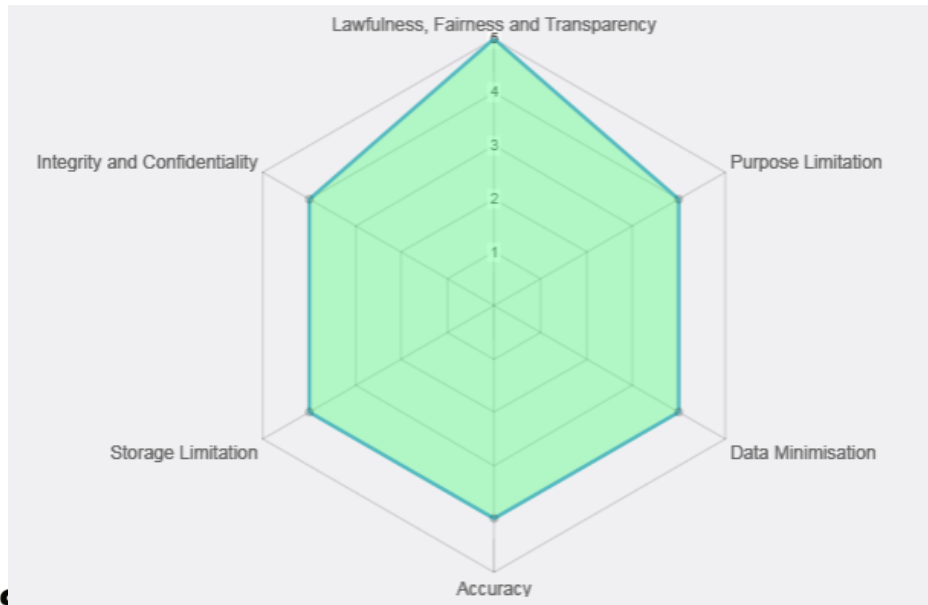
- PIAs are now a legal requirement!
- Support for PIAs and Privacy-By-Design just one element of GDPR compliance
- **BUT....**
 - PIAs firstly about ensuring that **rights and freedoms of individuals** are respected when processing their data or assessing individuals in some way.
 - Concerns as a by-product
 - Compliance with the law
 - Any impacts on the organisation(s) involved.



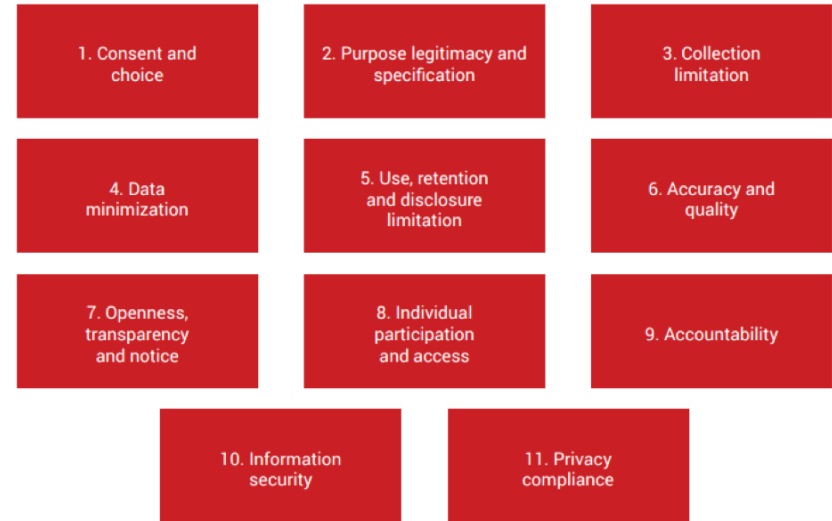
Are PIAs just about GDPR compliance?

- However, PIAs and GDPR Compliance activities both focus on ensuring appropriate treatment of **key principles of data protection**

GDPR (Article 5)



ISO 29100



PIA Requirements under GDPR

- **Article 35** - Data protection impact assessment
 - High risks to individuals exist? (1,3,4)
 - Nature/format of PIA? (7)
 - Seek relevant views, advice, codes of conduct, review (2, 8, 9, 11)
- **Article 36** - Prior consultation
 - If there are 'significant' residual risks from a PIA, consultation with authority required
- **Article 25** - Data protection by design and by default
 - PIA should be carried out "prior to the processing" in line with this principle
- Key recitals - 75, 84, 89-93

What is regarded as a “valid” PIA approach under GDPR?

Criteria	Where in GDPR
Systematic description of processing provided	Article 35 (7)(a)
Necessity and proportionality of processing considered	Article 35 (7)(b)
Risks to individuals are assessed/identified	Article 35 (7)(b) Recital 84, 90
Stakeholders are involved where necessary	Article 35 (2) Article 35 (9)

When is a PIA Necessary?

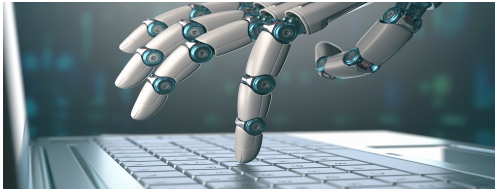
- Key GDPR sections
 - Art 35 (1),
 - 35 (3a-c),
 - Recitals 71, 75, 91

- Regulatory landscape still early and moving on this!
 - Regulation will require supervisory bodies to communicate a list of operations that require a DPIA - Art 35(4)... as well as exceptions that may be exempt



Test 1 – Evaluation, Scoring, Automated Decision Making

1. Does your scenario involve processing where evaluation, scoring, or automated decision making is made on specific individuals?



Scenarios?

Bank screening customers against credit reference database



Company tailoring special offers/deals based on spending or credit history, to the exclusion of some "bad" customers

Recitals 71,91 – examples:

Work performance/appraisal
Economic status
Health
Credit/spending habits
Personal preferences/interests
Behavioural characteristics

Refusing/limiting access to a service, or entry into a contract?

Test 2 – Monitoring

2. Does the scenario involve processing used to monitor or control data subjects?



Scenarios?

CCTV use in public areas a common example

Monitoring of employee computer use in the workplace

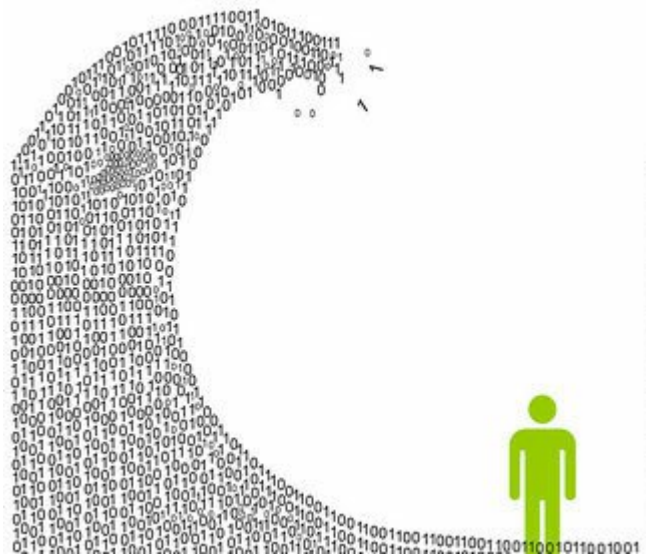
“Systematic” in nature – prearranged, methodical, in accordance with a plan, strategy, system

Key PIA issues – Who is monitoring? What for?
What if I can’t opt-out?

Physical as well as informational privacy

Test 3 – “Large Scale” Processing

3. Would the processing be regarded as “large scale” - in that a large number of data subjects are involved, a large range of different data items are processed, the processing occurs for a long duration (or permanently), or involves a large geographical area?



Recital 91....

How many people?

Volume of data?

Range/scope of data categories?

Duration? (permanent?)

Geographical extent?

Test 4 – Data Matching/Aggregation

4. Does the scenario involve processing where personal data is matched from two or more sources that would exceed the reasonable expectations of the data subject?



Cannot combine two different data sources, originally collected and used for separate purposes

Separate legal basis (e.g. consent) necessary for new combined dataset

Fundamental basis of “purpose limitation” principle

E.g. data sharing initiative between two organisations where new combined data is produced

Test 5 – Vulnerable/Disadvantaged Data Subjects

5. Does it include scenarios where data subjects are vulnerable or disadvantaged in their ability to query or dispute the data processing?



Scenarios?

Where “power imbalance” exists between controller and data subject

Employee -> employer

Nursing home -> elderly (sick) person

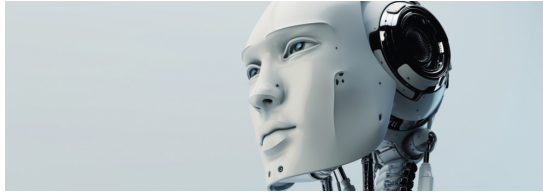
Hospital -> sick patient

School -> underage pupils (minors)

PIA should investigate that data collection method use addresses this advantage/imbalance and that any processing is not abusive of it

Test 6 – New/Emerging Technologies

6. Are new technologies previously not used by the core organization(s) used and relevant in the scenario, in a manner that could be regarded as privacy intrusive?



Does the technology introduce new (unforeseen) forms of data collection, usage, processing?

Are there appropriate measures in place to limit such usage (technical, procedural?)

Are stakeholders aware of these potential impacts? (role of PIA is to make them aware of risks)

Are they transparent about such impacts with data subjects?

More recent example – Deepfakes – what's next?



Test 7 – Accessed by “new” individuals?

7. Will any of this information be provided to “new” individuals who did not have routine access to it previously?

Outsourcing/re-delegation of particular collection/processing activity?

Any consequences/impacts (violation of codes of conduct?)

If YES, assurance of safe and secure principles in place around that new party are essential

Only sharing/delegating what is necessary??
Proportionality of processing maintained?

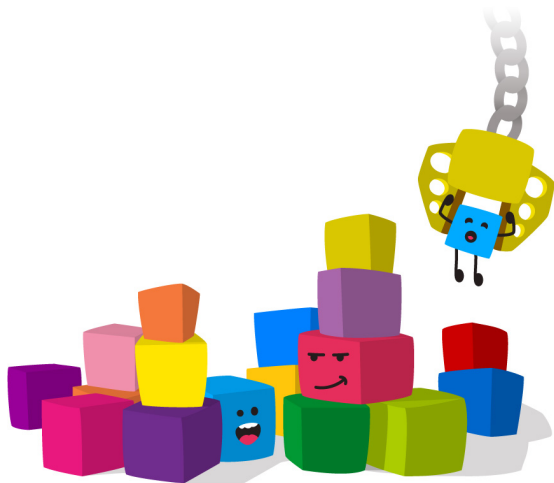
Good PIA example of such a scenario:

https://www.hiqa.ie/system/files/HI_PIA_Sample_Report.pdf



Test 8 – Collection of “new” data about individuals?

8. Does the scenario involve collection of new data about individuals not already collected, and used in a manner that could be regarded as privacy intrusive?



Consents in place (if applicable), notification information updated?

Potential for new add-on processing/matching/aggregation considered?

Data minimisation measures in place to reduce risk?

Test 9 – Minors

9. Does the scenario involve collection of data from minors under the age of 16?



Power imbalance principle applies

Ensure appropriate parental consent (or nearest guardian)

Ensure background check of parental source as part of collection/consent

Test 10 – Sensitive Data

10. Are any sensitive categories of data processed as part of the scenario - involving data collected directly from individuals or from other sources? (see Article 9 of GDPR for examples of key sensitive categories)



Tight definition: Categories in Article 9 of GDPR

Key examples of sensitive personal data include data relating to:

Racial or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Genetic data

Biometric data (including biometric photographs leading to unique identification such as biometric passport)

Health data

Sex life

Sexual orientation

Test 10 – Sensitive Data

10. Are any sensitive categories of data processed as part of the scenario - involving data collected directly from individuals or from other sources? (see Article 9 of GDPR for examples of key sensitive categories)



Others that may fall into scope?

Electronic communication data

Location data

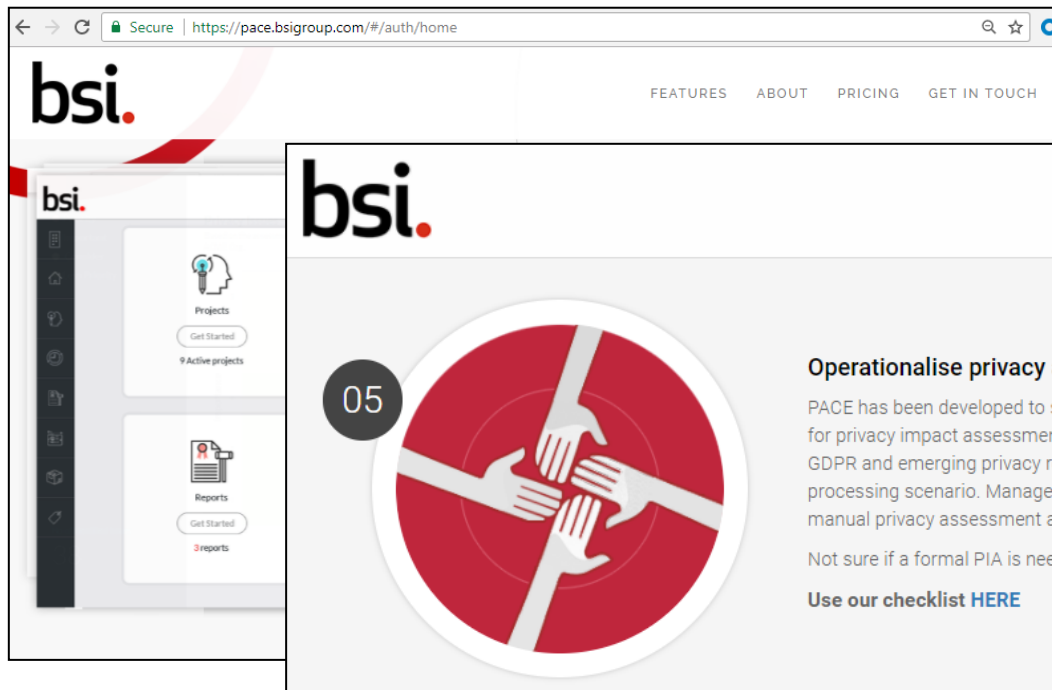
Financial data

Other “intrusive” data – personal documents, diaries, e-readers, note takers etc

If data is already made publically available – less likely to be regarded as sensitive

BSI Checklist Available – Is a PIA Required?

<https://pace.bsigroup.com>



bsi.

Privacy Assessment Coverage Engine (PACE)

Is a formal Privacy Impact Assessment (PIA) needed for your project/scenario?

As a rule of thumb, answering Yes (or Don't know) to **TWO** or more of the questions below indicates that processing is potentially high risk in nature.

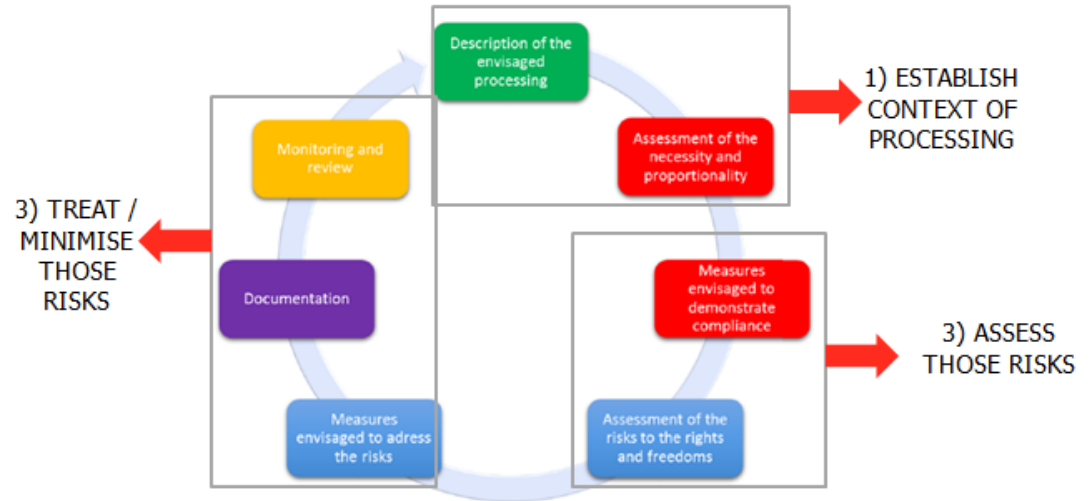
In such cases, a more complete assessment of privacy impact using one of the PACE assessment options available is strongly advised.

1. Does your scenario involve processing where evaluation, scoring, or automated decision making is made on specific individuals?
2. Does the scenario involve processing used to monitor or control data subjects?
3. Would the processing be regarded as "large scale" - in that a large number of data subjects are involved, a large range of different data items are processed, the processing occurs for a long duration (or permanently), or involves a large geographical area?
4. Does the scenario involve processing where personal data is matched from two or more sources that would exceed the reasonable expectations of the data subject?
5. Does it include scenarios where data subjects are vulnerable or disadvantaged in their ability to query or dispute the data processing?
6. Are new technologies previously not used by the core organization(s) used and relevant in the scenario, in a manner that could be regarded as privacy intrusive?
7. Will any of this information be provided to "new" individuals who did not have routine access to it previously?
8. Does the scenario involve collection of new data about individuals not already collected, and used in a manner that could be regarded as privacy intrusive?
9. Does the scenario involve collection of data from minors under the age of 16?
10. Are any sensitive categories of data processed as part of the scenario - involving data collected directly from individuals or from other sources? (see Article 9 of GDPR for examples of key sensitive categories)

Completing a PIA

- Risk Management 101 (ISO 31000...)

1. Establish the context
2. Assess the Risks
3. Treat the Risks



Completing a PIA – Step 1 - Establish the Context

So upon determining that a PIA is necessary... need to describe and characterise the processing.

- What (personal) data is being processed?
- In what way and for what purposes?
- Is that processing necessary?
- Is it proportional and fair?
- Riskiness of processing? Degree of technology use? Level of external party involvement?
- Clarity on the legal basis (one or more) for processing in the scenario?
- Are we compliant with any guidelines or relevant codes of conduct?

Use appropriate question checklist to support establishing context

Spreadsheet/tool options available

PACE PIA Checklist Support – Project Summary

bsi.

Privacy Assessment Coverage Engine (PACE)

Is a formal Privacy Impact Assessment (PIA) needed for your project/scenario?

As a rule of thumb, answering Yes (or Don't know) to **TWO** or more of the questions below indicates that processing is potentially high risk in nature.

In such cases, a more complete assessment of privacy impact using one of the PACE assessment options available is strongly advised.

1. Does your scenario involve processing where evaluation, scoring, or automated decision making is made on specific individuals?
2. Does the scenario involve processing used to monitor or control data subjects?
3. Would the processing be regarded as "large scale" - in that a large number of data subjects are involved, a large range of different data items are processed, the processing occurs for a long duration (or permanently), or involves a large geographical area?
4. Does the scenario involve processing where personal data is matched from two or more sources that would exceed the reasonable expectations of the data subject?
5. Does it include scenarios where data subjects are vulnerable or disadvantaged in their ability to query or dispute the data processing?
6. Are new technologies previously not used by the core organization(s) used and relevant in the scenario, in a manner that could be regarded as privacy intrusive?
7. Will any of this information be provided to "new" individuals who did not have routine access to it previously?
8. Does the scenario involve collection of new data about individuals not already collected, and used in a manner that could be regarded as privacy intrusive?
9. Does the scenario involve collection of data from minors under the age of 16?
10. Are any sensitive categories of data processed as part of the scenario - involving data collected directly from individuals or from other sources? (see Article 9 of GDPR for examples of key sensitive categories)

Privacy Impact Assessment (PIA)

Not sure if a formal PIA is needed for your scenario? Use our checklist [HERE](#)

Privacy Impact Assessment (PIA) Scenario Check (Detailed)		Gain detailed privacy profile of individual project scenarios as part of existing Privacy Impact Assessment (PIA) procedures. Maximum 130 Questions approx.	?
Privacy Impact Assessment (PIA) Scenario Check (Summary)		Gain summary privacy profile of individual project scenarios as part of existing Privacy Impact Assessment (PIA) procedures. Maximum 50 Questions approx.	?

Reset Back Next

Steps: 1 2 3 4

Project Setup

Information provided in this section helps identify an appropriate set of questions based on the nature of the data processing activity being tested.

Project Details

Full Name: _____ Short Name*: _____
(max 12 characters)

Organisation Details

Full Name: _____ Short Name*: _____
(max 12 characters)

Overview: _____
Please provide a broad description of the scope and objective of Project 01, as well as anything else you feel is relevant.

*Mandatory fields - shortname provided above for project and organisation are referred to throughout the assessment.

Reset Next

<https://pace.bsigroup.com/>

PACE PIA Support – Structured “Scenario Check” Questions



Secure | <https://pace.bsigroup.com/#/p>

bsi / Dashboard / Projects

6%



Summary of Privacy Impact Factors

Particular privacy impact factors in relation to data, technology and external party use for OPTion 5 are highlighted below



Data Use

The scope and nature of the data processing in this scenario increases the impact and importance of key privacy compliance risks identified in this report. In particular that:

- › Data regarded as sensitive personal data is being processed in OPTion 5
- › New data about individuals is being collected, and could be processed in a manner regarded as privacy intrusive
- › New processing in relation to typical processing of personal data will occur in OPTion 5
- › Currently unknown follow-on processing will be required, or is expected in the future
- › OPTion 5 data relates to research purposes
- › Data is collected from minors as part of OPTion 5



External Party Use

The involvement of external parties in this scenario also increases obligations to ensure that relevant data processing is valid from legal and compliance perspectives. Factors increasing risk impacts that relate to use of external parties include:

- › Technologies may be used by external parties in the processing of data relevant to OPTion 5
- › External parties will be involved in the processing of sensitive personal data, or special categories
- › Personal data will be transferred to these external parties
- › Personal data will be stored by external parties, in IT systems or other physical means
- › External third parties intend on using other external parties to support OPTion 5 processing
- › If external parties are involved in this research or scientific based processing this could also increase privacy impact



Technology Use


The scope and nature of technologies used also increases risk around data processing legitimacy and compliance requirements, hence the need for such processing to be managed appropriately. Areas increasing such technology-use impacts include:

- › IT systems are used in the processing of data
- › Cookies or other tracking technologies are used
- › The fact that new software systems are being developed in OPTion 5
- › Advanced technologies are being used to determine specific characteristics of persons whose data is being processed. Such processing activity needs to be managed and monitored carefully in line with legal requirements around such data processing
- › The fact that external parties are involved in processing
- › New software systems are being developed in OPTion 5 which will involve external third party developers

Other laws beyond data protection allow (or require) us to collect some or all of the relevant data

Completing a PIA – Step 2 - Assess the Risk

What kinds of risk??

1. Legal impacts/non-compliance
 - Standardised (ala a gap assessment)
- 
2. Impacts on the individual or organisation
 - Nuanced/bespoke/trickier to identify
 - Understand specific relationship between individual and org!

Assurance that risk assessment is thorough? Systematic?
Covers all areas? And both concerns (1) and (2) above?

Use foundational privacy principles as a guide



WHO?

DPO/Compliance/Risk
Data Owners/Handlers
Data subjects?
DP Supervisory authorities?
IT/Legal/HR?

PIAs -> Linking Compliance Risk to Impact on Persons

Compliance/Technical Concern	Individual(s) concern?
Inadequate disclosure controls	➔ Is my info being shared inappropriately
Data use has changed over time	➔ Is my data being used for other purposes that I know nothing about?
New surveillance/monitoring	➔ Is my privacy being intruded
Merging of data	➔ Do they have more info on me than I'd like them to have?
Collection or linking of multiple ID points	➔ Am I able to truly use service X anonymously?
No retention/deletion procedures	➔ Why are they still contacting me/using my data?

PACE PIA Support – Step 2 - Assess the Risk



	Scenario Profiling <input checked="" type="checkbox"/> >
	Collection, Processing, Usage <input checked="" type="checkbox"/> >
	Accessibility, Transfer and Data Lifecycle <input checked="" type="checkbox"/> >
	Procedures, Notices, Requests, Complaints <input checked="" type="checkbox"/> >
	Security and Privacy Measures <input checked="" type="checkbox"/> >

bsi / Dashboard / Projects

100%

Filter

In relation to automated decision making or profiling:

Question 29

We have explicit procedures or mechanisms in place that limit the ability to easily link or aggregate personal data records with each other, and/or with other external sources of data that increase the ability to uniquely identify individuals

"YES - Fully Addressed"

"Partially Addressed"

"NO - Not Addressed"

Does Not Apply

Comments

Assign question to stakeholder

Reset

Save

Skip

Back

Next

Generate Report

PACE PIA Support – Step 2 - Assess the Risk

Lawfulness, Fairness and Transparency

Privacy Issues Report

In order to mitigate key reduce or remediate key privacy compliance risks, the following broad areas of remediation are recommended.

Sort By: Rating Probability Importance

Issue	Overview	Rating	Probability	Importance	Action
1 Data Transfer Controls	This concern area considers appropriateness of measures and controls that protect transfers of personal data between LONG 19 Test stakeholders	Priority	5	4	View
2 Security Risks and Controls Measures	This area considers evidence that information security risks and mitigating controls are identified and implemented for LONG 19 Test. Appropriate security controls ensure confidentiality, integrity and availability of LONG 19 Test data, and should exist at operational, functional and strategic levels.	Priority	5	4	View
3 Data Access to Persons - Controls	This area considers evidence that specific data access controls are in place that restrict key LONG 19 Test data to those who need to access it, in line with "need to principles" of security and data protection.	Priority	5	4	View
4 Access Admin Measures	Aside from specific data access controls, this area specifically considers evidence that appropriate access admin policies and procedures are in place to support effectiveness of such specific controls on an ongoing basis.	Priority	5	4	View
5 Security Complianc Measures	This risk area considers evidence that any LONG 19 Test information security management system, identified risks, implemented controls, policies and procedures are assessed on an ongoing basis by an appropriate impartial security professional, either internally or externally as appropriate, as a foundation for LONG 19 Test security compliance assurance.	Priority	5	4	View

38

Completing a PIA – Step 3 - Treat the Risk(s)



Generic ->context-specific privacy risks,

Risk prioritisation/scoring method

Plan/Implement fixes....

Consider cost/benefit of each...

ARE THERE RESIDUAL RISKS?



COMMON FIXES?

Minimise or **reduce** personal data collected/processed?

Improve or update **communications** or notifications to individuals?

Improve **opt-in** mechanisms for collection, improve collection transparency

Improve **safe and secure** mechanisms (2FA, encryption, anonymization etc)

Data owners/handlers - **training** + awareness

PACE Support – Treat the Risk(s)



Remediation Guidance

Key remediation controls to consider to reduce or eliminate this risk include

Broad Measures to Consider

Transfers: Establish and enforce appropriate controls to protect data transfer flows between [Project] stakeholders and external parties if applicable

More Specific Measures to Consider

Data Transfer Procedures + Mechanisms

- › In defining an appropriate approach, transfers of personal or sensitive personal data should be governed by rules set out in **LONG 19 Test** policy and evidenced by an appropriate legal basis.
- › Examples of an appropriate legal basis for such transfers includes (1) Consent, (2) Standard Contract Clauses, (3) Binding Corporate Rules, (4) Codes of Conduct or other form of agreement in line with legislation and regulations of **LONG 19 Test** processing jurisdictions

Secure Transfer Agreements

- › Develop and maintain formal agreement / contracts governing the secure transfer of information within the organisation and between the organisation and third parties
- › Identify and select appropriate legal transfer mechanisms govern the transfer of data within and out of the organisation
- › Assign an individual with responsibility for monitoring the legal transfer of personal data

Transfer Policies and Procedures

- › Seek advice in developing appropriate data transfer policies and procedures. A priority is to include appropriate notice information to data subjects whose personal or sensitive data will be transferred as part of **LONG 19 Test**
- › Other key elements in a detailed personal data transfer policy include (1) setting out the types of personal data transferred and legal basis on which it is permitted, (2) details of where and to what external parties data has been transferred to, including provisions for organisational and technical measures to ensure data protection measures
- › Ensure that procedures are shared and communicated with any relevant data handlers or stewards involved in such transfers.

Linking PIAs with project/program management

Need to build into project lifecycles. A PIA is **not just a checklist!**

Senior-level **buy-in** is key (especially for key projects)

Conduct **early in the project** (in line with official GDPR definition)

Train PM teams up with principles of PIAs + their operation

Scale the **scope/detail of the PIA** to the nature of the project (e.g. short vs. long questionnaires!)

Develop clear PIA **decision gates**

- (1) PIA Screen - Go/No-Go
- (2) Proceed with project based on PIA findings?
 - External consultation necessary?
- (3) Repeat PIA at later point?



Linking PIAs with project/program management



PIA Risk Treatment

Add to overall **project risk register**

Add risk treatments/remediations as regular items in **project plan**

Decide what risks are accepted (**and who accepts the risk?**)

Decide whether PIA findings are **published/shared/redacted** etc?

Store the PIA outcomes securely....

References + Further Info

Article 29 WP Guidelines on DPIAs

- ec.europa.eu/newsroom/document.cfm?doc_id=44137



ARTICLE 29
Data Protection Working Party

ICO – Conducting Privacy Impact Assessment Code of Practice

- <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>



References + Further Info

New Zealand Privacy Commissioner – How to Do a Privacy Impact Assessment

- <https://www.privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Assessment-Part-2-FA.pdf>

BSI PACE (Privacy Assessment Coverage Engine) Software

- <https://pace.bsigroup.com>

contact: pace@bsigroup.com

The screenshot displays the BSI PACE software interface. At the top, the BSI logo is visible on the left, and navigation links for FEATURES, ABOUT, PRICING, GET IN TOUCH, LOGIN, and SIGN UP are on the right. The main content area features a 'Privacy Coverage Profile' radar chart. Above the chart is a table with the following data:

Organisation	Project	Updated on	Assessment Name	Assessment Category	Framework
ACME Org	ACME Overall	14 Oct 2017	QMS 91 Rev	Detailed Assessment	EU GDPR Compliance Check (External)

The radar chart is titled 'Privacy Coverage Profile' and 'GDPR Coverage Rating - BS10012 Key Principles (Out of 5)'. It shows coverage levels for 12 key principles: Leadership, Planning, Support; Performance and Improvement; Key Appointments; Identifying + Recording Uses of Personal Information; Risk Assessment and Treatment; Training and Awareness; Privacy Management Updates; Fair and Lawful Processing; Processing for Specific Legitimate Purposes; Adequacy and Data Limitation; Data Accuracy; and Data Retention and Disposal. A green shaded area indicates the current coverage level for each principle. To the right of the chart, there is a 'GDPR Compliance Support' section with the text: 'Assess your organisation's data use against privacy regulations and best-practice - EASILY, EFFICIENTLY & SCALABLY.' A large red circular button with white text says 'SIGN UP HERE to complete an assessment'.

Q+A

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