# Privacy By Design (PBD) Principles

# Brunel University London

***An ISO/IEC 27001:2013:*** *Aligned Document - Implementing Cyber and Information Security Best Practice*

**Mick Jenkins**
Chief Information Security Officer

# Document History

| Version | Author | Comments | Date |
|---|---|---|---|
| V 0.1 | Andrew Clarke | Initial Draft | 04/06/2019 |
| V 1.0 | Andrew Clarke | Approved CISO & DPO | 26/06/2019 |
| | Andrew Clarke | Annual Review | 08/06/2020 |
| | | | |
| | | | |
| | | | |
| | | | |

### Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

| | |
|---|---|
| Owner: Michael Jenkins | Chief Information Security Officer |
| Signature: MGJ | Date: 26 Jun 2019 |
| Approver: Pekka Kahkipuro | Chief Information Officer |
| Signature: PK | Date: 26 Jun 2019 |
| Distribution: | |
| | |
| | |
| | |
| | |
| | |

This document requires the approval from BUL as defined in the ISMS Compliance document.

# Contents

# 1. About this document

## 1.1 Purpose of Document

Brunel University is committed to safeguarding its information and computing infrastructure upon which the teaching and research functions rely. Additionally, the University is strongly committed to maintaining the security and privacy of confidential personal information and other data it collects or stores.

In order to guide the University community in achieving these objectives, the University adheres to the Privacy By Design (PBD) philosophy.

Privacy By Design, in IS terms, means that the deployment of both hardware (infrastructure architecture) and services (software architecture) has been designed from the foundation to be secure. Security by Design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as standard Privacy builds, continuous testing, authentication safeguards and adherence to best programming practices.

The University has a formal Vulnerability Management Programme (VMP) to bring in industry good practice set against our risk management process to maintain the PBD principles.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

## 1.2 Responsibilities

Table 1 – responsibilities

| Title / Role | Description |
|---|---|
| All | Responsible for adhering to the PBD principles |

## 1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

| | |
|---|---|
| University ISMS Control Number | SOA – Number A14 – System acquisition, development and maintenance |
| ISO 27001:2013 Conformance Control | Information Classification Objective<br>A.14.1.1 Information security requirements analysis and specification |

## 1.4 Scope

The scope of these Principles apply to:

- Any server or client that IS manages or is responsible for, including servers which are managed by third parties on behalf of IS.
- Any server or client that College IT manages or are responsible for, including servers which are managed by third parties on behalf of Colleges.
- Any software on these servers or clients. In this document, “software” shall be taken to include firmware, BIOS, hypervisor, operating system, driver, library, middleware, application, service, and other digital capabilities.
- All public-facing Cloud systems and services that the University subscribes to including PaaS, SaaS, and IaaS.

## 1.5 Principles Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

## 1.6 References

BUL Change Control Process (ISMS 12.1.2)
BUL-POL-12.6 - Vulnerability Management
BUL-POL-12.6 - Patch Management
BUL-PR-14.09 - Secure By Design Principles

## 2.0 Privacy By Design Principles

**"Privacy by Design" and "Privacy by Default"** is an architectural and strategic approach to projects that promotes privacy and data protection compliance, and helps you comply with the Data Protection Act 2018 (DPA).

The Information Commissioner's Office (ICO) encourages organisations to seriously consider privacy and data protection throughout a project lifecycle, including when:

- Building new IT systems to store or access personal data;
- Needing to comply to regulatory or contractual requirements;
- Developing internal policies or strategies with privacy implications;
- Collaborating with an external party that involves data sharing; or
- Existing data is used for new purposes.

**Privacy by design and the GDPR**

The EU General Data Protection Regulation (GDPR) is incorporated into the DPA 2018. Article 25 of the GDPR, "[d]ata protection by design and default", requires you to "implement appropriate technical and organisational measures" throughout your data processing project. As such, data must be considered at the design stage of any project, during which you must process and store as little data as possible, for as short a time as possible.

Privacy by design is an essential method to systems architectural design that consider privacy throughout the whole design process. This concept is similar to value sensitive design, such as human values are taken into account in a precise manner during the whole procedure.

Privacy by design is a particular approach to projects that endorses data protection and privacy compliance from the beginning. This method is essential for compliance with the Data Protection Act, and it will assist the University to conform to our obligations under the legislature

Benefits of Privacy by Design
Privacy by design is an essential tool to reduce privacy risk and build trust. Creating systems, products, processes and projects with privacy at the outset can lead you to numerous benefits, such as:

- Identify potential problems at early stage and address these problems easily promptly
- Increase the awareness of data protection and privacy across the University
- Meet legal obligations instead of breaching Data Protection Act.

## 2.1 Seven Foundation Principles

1. Preventatives not counteractive and Pre-emptive not reactive
2. Privacy as default setting
3. Embedded privacy in design
4. Full functionality: positive-sum instead of zero-sum
5. Transparency and visibility: keep it exposed
6. Endwise security and full lifespan protection
7. Respect for the privacy of user and keep it user-centric

Principle 1: Proactive not reactive: preventative not remedial

The Privacy by Design (PBD) framework is characterised by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur. PBD does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred —it aims to identify the risks and prevent the harms from arising. In short, PBD comes before-the-fact, not after

Principle 2: Privacy as the default setting

PBD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy —it is already built into the system, by default.

Principle 3: Privacy embedded into design

Privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality.

Principle 4: Full functionality: positive-sum, not zero-sum

PBD seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through the dated, zero-sum (either/or) approach, where unnecessary trade-offs are made. PBD avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both.

Principle 5: End-to-end security: full lifecycle protection

PBD, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved —strong security measures are essential to privacy, from start to finish. This ensures that all data are securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PBD ensures cradle to grave, secure lifecycle management of information, end-to-end.

Principle 6: Visibility and transparency: keep it open

PBD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. The data subject is made fully aware of the personal data being collected, and for what purpose(s). All the component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify!

Principle 7: Respect for user privacy: keep it user-centric

Above all, PBD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. The goal is to ensure user-centred privacy in an increasingly connected world. Keep it user-centric.


1
Proactive not reactive – preventative not remedial
Anticipate, identify and prevent invasive events before they happen; this means taking action before the fact, not afterward
2
Lead with Privacy as the default setting
Ensure personal data is automatically protected in all IT systems or business practices with no added action required by any individual
3
Embed privacy into design
Privacy measures should not be add-ons but fully integrated components of the system
4
Retain full functionality (positive-sum, not zero-sum)
Privacy by Design employs a "win-win" approach to all legitimate system design goals; that is, both privacy and security are important and no unnecessary trade-offs need to be made to achieve both
5
Ensure end-to-end security
Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed
6
Maintain visibility and transparency – keep it open
Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification
7
Respect user privacy – keep it user-centric
Keep things user-centric, individual privacy interests must be supported by strong privacy defaults, appropriate notice and user-friendly options