

1 Scope

The term “Privacy by Design” means nothing more than “data protection through technology design”.

Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created. The principle of Privacy by Design, which is in the General Data Protection Regulation (GDPR) the current approach in the data protection guidelines, which requires persons responsible already to include definitions of the means for processing at the time that they are defined in order to fulfil the basics and requirements of Privacy by Design. Legislation leaves it completely open which exact protective measures are to be taken by Aseptika.

Aseptika’s projects and clinical trials, which may impact privacy and data protection, are subject to a Privacy Impact Assessment (PIA) and a Data Protection Impact Assessment (DPIA) at an early stage of the project and then throughout its lifecycle.

For example, when Aseptika is:

- Building a new IT system for storing or accessing personal data.
- Developing legislation, policy or strategies that have privacy implications.
- Embarking on a data sharing initiative.
- Product delivery into another organisation, such as the NHS or Local Government Authority.
- Using data for new purposes.
- Developing a new medical device.

2 Responsibilities

Aseptika’s SIRO is responsible for ensuring a DPIA and PIA screening questionnaire (ASL IG F-001 Privacy Impact Assessment PIA and ASL IF F-022 Data Protection Impact Assessment DPIA) are undertaken to determine if a full PIA and DPIA’s will be reviewed at the product/project review meetings.

3 Procedure

The PIA and DPIA will be conducted following the Information Commissioner’s Office Code of Practice using the Annexes to record the outcomes and if a PIA/DPIA is required.

Aseptika documentation, such as data flow maps and asset registers will be updated accordingly.

Specialist privacy advice must be sought if required.

4 References

| | |
|--------------------------|---|
| ISO/IEC 27001:2022 | Information security, cybersecurity and privacy protection — Information security management systems |
| BS EN ISO/IEC 27701:2021 | Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management |
| ISO 27033-6 IEC/EN 2016 | Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access |
| ISO/IEC 27001:2022 | Information security, cybersecurity and privacy protection — Information security management systems |

| | |
|--------------------------|---|
| BS EN ISO/IEC 27701:2021 | Information Security Techniques - Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management |
| WCAG 2.1 | Web Content Accessibility Guidelines 5 June 2018 |
| NHSx DTAC | Digital Technology Assessment Criteria |
| NHS | The Information Security Management: NHS Code of Practice April 2007 |
| NHS DSPT | NHS Data Security & Protection Toolkit |
| Cyber Essential | Cyber Essentials & Cyber Essentials Plus |
| ICO.org | Personal data breaches: Information Commissioners Office |
| ICO.org | The Information Commissioner's Office (ICO) Guide to Data Protection |
| MDCG 2019-16 Rev.1 | Guidance on Cybersecurity for medical devices |

5 Document History

| Version | Date | Authors Initials | Reviewers Initials | Changes from Previous Version | Authorised by & date |
|---------|------------|------------------|--------------------|--|-----------------------------------|
| 1.1 | 12.02.2018 | GL | | First Draft | |
| 1.2 | 14.02.2018 | CAA | | Update to new format | |
| 1.3 | 15.02.2018 | CAA | | Formatting | |
| 1.4 | 16.02.2018 | JMA | | Updating | |
| 1.5 | 03.05.2018 | ETRA | | Update to a new template and a new document number | |
| 2.0 | 11/12/2018 | ETRA | CAA, JAA, CB | Annual review and part of CC2018-0187 | |
| 3.0 | 02.12.2019 | JA | MP | MDR Transition update, part of CC2019-057 | Kevin Auton |
| 4.0 | 29.10.2020 | JA | MP | Update as per 2020-059 | CAA |
| 5.0 | 22.11.2021 | JA | GE | Annual update CC2021-075 | Kevin A Auton 23.12.2021 |
| 6.0 | 07.03.2022 | JA | GE | Update language CC2022-018 | Kevin Auton 18.03.2022 |
| 7.0 | 24.06.2022 | JA | GE | Update Policy CC2022-041 | CAA 04.07.2022 |
| 8.0 | 27.10.2022 | JA | GE | Migrate to AWS CC2022-063 | CAA authorise JA 02.11.2022 |