Document name:	Document type:	Version:
Overview of Medicover Information Security Program	Guideline	1.2
Approved by:	Document owner:	Date of approval:
CEO	CIO	

Overview of Medicover Information Security Program

Document name:	Document type:	Version:
Overview of Medicover Information Security Program	Guidelines	1.2
Approved by:	Document owner:	Date of approval:
CEO	CIO	

Content

Document name:	Document type:	Version:
Overview of Medicover Information Security Program	Guidelines	1.2
Approved by:	Document owner:	Date of approval:
CEO	CIO	

1 Introduction

1.1 Medicover has established and implemented a Medicover Information Security Policy (MISP) together with Medicover Personal Data Protection Policy (Privacy Policy) which are internally available to all employees, and which must be followed by those employees.

The following information provides a selective overview of some of the main provisions and objectives of the MISP, Privacy Policy and Medicover Cybersecurity and Privacy Program.

2 Cybersecurity

2.1 IT Security / Cybersecurity Governance
Medicover has implemented a comprehensive Information Security Management System across the entire company. The Information Security Management System is based on ISO 27001. Several of Medicover's subsidiaries are already ISO 27001 certified.

Cybersecurity governance consists of corporate structures (led by the Chief Information Security Officer, who reports to the CIO). Major decisions about cybersecurity are discussed during regular meetings of the cybersecurity committee in which cybersecurity representatives of each business unit participate.

2.2 Executive management reporting is provided by corporate structures to the Executive management team (EMT).

2.3 Medicover Information Security Policy

Medicover Information Security Policy sets forth cybersecurity framework in Medicover, defines applicability of cybersecurity framework and describes roles and responsibilities in cybersecurity.

Detailed information security requriements are provided in the MISP appendix: the Medicover Information Security Standard which provides information security requirements in following sections:

1. Information risk management
2. Human resources security
3. Asset management
4. Access Control
5. Cryptography
6. Physical and environmental security
7. Operations security
8. Communications security
9. System acquisition, development and maintenance
10. Supplier relationships
11. Information security incident management
12. Information security aspects of business continuity management
13. Compliance
14. Cloud security

2.4 Key Cybersecurity Programs

The Cybersecurity has established key cybersecurity programs which address the most important cybersecurity challenges, including but not limited to:

- Endpoint Detection and Response solutions which secure Medicover against suspicious and malicious threats.
- Security Operation Center which provides a 24/7 cybersecurity monitoring service for each Business Unit.
- Firewall and IPS services to ensure protection from network threats
- Vulnerability management program which aims to periodically check the IT environment in each Business Unit for vulnerabilities and manage the remediation.
- Security testing for key assets and infrastructure that simulate cyber-attacks.
- Web security program that aims to improve security of publicly available web application and sites, through secure SDLC (Software Development Life Cycle), web applications security testing, and Web Application Firewall (WAF) deployment,
- Data protection is based on Data Leak Prevention system to monitor and actively block fraudulent data transfers that may occur on corporate devices, Mobile Device Management to enforce security policies on enterprise mobile devices and encryption techniques.

2.5 Training

Cybersecurity provides regular awareness communication based on current threats, and also provides regular social engineering tests targeted at employees from all business units.

Each Medicover business unit provides information security & privacy training with key security and privacy matters.

2.6 Security Incident and data breach response

Incident response procedures are in place. Every business unit is responsible for establishing and operationalizing incidents and breach management processes. Processes are aligned with GDPR and NIS requirements and breaches are reported to the regulators whenever required by law. Breaches and the underlying root causes are regularly reported to management and improvements are planned and implemented.

3 Privacy Policy

3.1 Privacy Policy Systems and Procedures

Medicover has established Medicover Personal Data Protection Policy (Privacy Policy) together with Medicover Personal Data Protection Standards (Privacy Standards) which have been implemented within Medicover companies. The Privacy Policy and Privacy Standards apply to the entire operation, including suppliers.

Privacy Policy provides the most important rules for personal data protection to be followed by every employee in Medicover, where Privacy Standards set forth minimum requirements for Medicover companies for privacy management and documentation. Each local business unit has also established a local privacy documentation and policies to describe in detail how data protection is maintained in local processing activities, including lawful processing, transparency, fulfilling subject rights, data processors' management, privacy by design and risk assessment.

3.2 Responsibilities

The Data Privacy Manager in the corporate cybersecurity function is responsible for providing support in cross-business projects to ensure compliance with privacy laws, and to define strategies for ensuring data privacy. This Data Privacy Manager is also responsible for overseeing the work of the Data Protection Officers ("DPOs"). DPOs are responsible for monitoring data privacy compliance in local business units.

3.3 Risk / compliance management.
The Data Privacy Manager and corporate cybersecurity function are responsible for defining risks and following up remediation plans for all Medicover entities and cross-business projects. They also support DPOs with defining risks and mitigation plans for local projects.

3.4 Disciplinary actions in case of breach
Medicover takes data privacy and information security very seriously and operates a zero tolerance policy. Each employee must follow the group and local procedures. Every policy breach is investigated and could be a reason for termination.

3.5 Audit of privacy policy compliance
The Cybersecurity Department performs an annual Privacy Maturity Self-Assessment with every business unit in the Medicover. The assessment provides agreed action plans for improvement. Some of Medicover's business units undergo independent external audits during the ISO certification process.

3.6 Customer Privacy Information
Each Medicover company provides all required information under articles 13 and 14 of the GDPR, or any other relevant data privacy laws for companies from outside EU.

All companies from EU provide their customers and all other data subjects for which personal data are processed with at least the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- legal basis for data processing;
- the recipients or categories of recipients of the personal data, if any (e.g. Medicover's providers and vendors or empowered authorities – but only if it directly required by a law);
- data transfers description;
- data subjects' rights;
- period of which the personal data will be stored.

Depending on local privacy regulations, business units provide their patients and customers with user-friendly ways to manage their privacy, for example:

- opt-in/opt-out features for marketing processing in patients' on-line accounts;
- cookie bars allowing transparent decisions for users about their cookies usage by Medicover;
- plain and transparent language in all privacy documents and consent wordings;
- clearly communicated ways for executing data subjects' rights, including but not limited to the right to be forgotten, data access rights, objections to data transmission.

Data subjects' requests are managed based on specific internal procedures which describe responsibilities and workflows for request processing to ensure respect for the subject's privacy.

3.7 Customer Privacy Complaints
Every business unit is responsible for the data subject rights' execution process and the data subject's complaints management process. Processes are managed first by the DPO and documented. Each request is processed within the timelines defined by the GDPR or other applicable privacy law.