DATA PROTECTION MANUAL
Information and Cyber Security Policies

iLOQ Oy

Last Modified: 11 November 2024

Contents

INTRODUCTION

This document contains iLQQ's most important information security policies. In addition to these policies, there are policies and instructions for different interfaces, such as the requirements for the supplier interface and the survey, as well as the information security manual for iLOQ's internal use.

The information security policy is a high-level description, where, for example, commitment and continuous improvement are described. The goal of the access management policy is to manage requests for information and data processing services and to ensure authorized users have access to systems, applications and services and to prevent unauthorized access. Device Management and Clear Desk and Screen Policy guides how we can prevent the loss, damage, theft or endangerment of property and the interruption of the organization's operations. The Information Transfer Policy describes the protection of information transferred within the organization or with an external party. The Cryptography Policy ensures the appropriate and effective use of cryptography in order to protect the confidentiality, authenticity and integrity of information. Personal data lifecycle describes the management of employee data at different stages of the employment relationship. The purpose of the privacy policies is to define the principles, operating methods and responsibilities to ensure the legal processing of personal data and a high level of data protection.

INFORMATION SECURITY POLICY

This Policy provides a framework for the information security objectives which align with iLOQ's purpose, values and strategic priorities. Information security objectives and their metrics are defined and monitored according to the annual plan. iLOQ complies with the requirements of ISO 27001:2022.

We observe and fulfil information security requirements regarding our products, software solutions and operations that are received from interested parties as well as those laid out by regulations, applicable laws, and other compliance criteria. We commit to satisfy applicable requirements related to information security. We ensure the confidentiality, integrity and availability of information about the organization and stakeholders.

Information security is developed continuously and systematically according to information security management system. We identify the information security risks and plan the needed actions and controls associated with our operation. Deviations detected and opportunities for improvement observed in our operations are handled openly and obtained information is utilized in continuous improvement of processes and methods. Information security is monitored and measured with the aid of operative and information security key figures as well as observed non-conformities. External providers' information security is also monitored.

The information security policy applies to all levels in the organization. We commit our personnel and stakeholders to conceal in their work assignments confidential information to be processed. Each employee is aware of their effect on information security always, and they are able to initiate and, where necessary, take preventive and corrective actions.

This Policy will be communicated and acknowledged to the whole organization and relevant interested parties through employee inductions, trainings and informal communication methods. The information security policies are reviewed annually and if significant changes occur.

ACCESS CONTROL POLICY

iLOQ access rights are limited by usernames and passwords. System usernames and passwords may not be disclosed to anyone. The username will be locked after a sufficient number of failed login attempts. In cloud services (email, Teams, etc.), the user is required to provide multi-factor authentication.

The user data master database is the AD. In SSO systems, user information is automatically updated from the AD. AD has forced password policies. SSO is the preferred MFA method in all services and applications.

Access controls are allocated on the basis of business need and 'Least Privilege'. Access to services and applications is prohibited unless specifically permitted. Personnel access rights are managed on a task-by-task basis by a supervisor and are managed in the Service and Application Register. The principles of access control are described in the Personal Data Lifecycle process.
The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) are restricted and controlled and not provided by default. The installation of workstation and server applications is monitored.

The source code of the products is stored in the version control systems. Access to the systems is controlled by person and role basis by version control system owner defined in Service and Application Register.

DEVICE MANAGEMENT AND CLEAR DESK AND SCREEN POLICY

An employee may only use iLOQ devices in their work. iLOQ devices are intended for use by iLOQ employees only and are intended for the performance of work tasks. Only software required for work tasks may be installed on iLOQ devices.

All iLOQ devices are registered and centrally managed. Devices are automatically updated using a management system. All workstations are protected by security software. Company information on the devices are encrypted. When an employee uses iLOQ devices, company information can be deleted if necessary. In situation when employees' employment contract ends, all devices must be returned according to Personal lifecycle and IT Procurement Processes. When agreed separately devices that are not returned must be removed from iLOQ Mobile Device Management System and the iLOQ data must be erased.

When an employee is outside the workplace network, he or she accesses the company network through a VPN. Untrusted network connection should be avoided. When using untrusted networks VPN connection is requested. Access to iLOQ email is encrypted. Logging in to public devices or services with iLOQ IDs is not allowed.

The company applies the principles of a clean table and display. iLOQ devices and removable storage media must not be left unattended and must be kept locked to prevent unauthorized access to the devices and information. iLOQ computers lock automatically after 15 minutes. The screen must always be locked when leaving the workstation. Privacy filters are used when performing work tasks in situations where outsiders can see internal or confidential information on the employee's screen. The organization avoids printing documents; special attention must be paid to the secure handling of printouts outside the workplace.

The data on the servers is backed up. User data is stored in iLOQ provided services i.e. OneDrive, SharePoint, M-Files where the data is automatically backed-up. Data is not preferred to be stored on local device.

INFORMATION TRANSFER POLICY

Networks are controlled by firewalls and IPS systems. Network services are ensured by SLAs. Own network devices are controlled by IT Manager. In addition to critical devices are under warranty. Servers and workstations are secured with malware detection system. Endpoints are monitored with EDR and NDR solutions. Server, management and DMZ networks are segmented to separate networks.

Communication between iLOQ's locations and remote workers is encrypted with VPN. Encrypted connection is used always in information transfer e.g. SSL. If sending classified information by email it must be encrypted. E-mail traffic is routed through the service provider's filters and iLOQ Oy's web and e-mail traffic is routed through a proxy server, where traffic is restricted, filtered and blocked.

CRYPTOGRAPHY POLICY

When using encryption, documented, and verified algorithms and implementations must be used. The following list shows the status of some popular algorithms. Vulnerable algorithms should be considered to be replaced in existing systems. Obsolete algorithms should not be used in new systems. The cryptographic algorithms recommended for application development are described in the Secured Software Development Manual (secret document).

Recommended algorithms should be used in new systems.

RC4 – vulnerable

MD5 – vulnerable

SHA-0 – vulnerable

SHA-1 – vulnerable

SHA-2 – recommended

Triple-DES – obsolete

Blowfish – obsolete

Twofish – obsolete

AES-128 – obsolete

AES-256 – recommended

RSA (under 2048 bits) – vulnerable

RSA (2048 bits or more) – recommended

ECC (384 bits for public key recommended)

Elliptic-curve Diffie–Hellman (ECDH) is a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. The key, or the derived key, can then be used to encrypt subsequent communications using a symmetric-key cipher.

The corporate network is protected by VPN solution. VPN connection security keys are managed by the IT Manager.

SSL certificates are managed on the external service provider's web portal by IT Manager. Certificates are valid for the period specified at the time of issue. The certificates are managed and renewed regularly.

If e-mail contains sensitive or valuable data, it must be encrypted by selecting “secret” label. Instructions for enabling email encryption are described in *iLOQ Information Security Handbook (turvallisuuskäsikirja).docx*

The data on all workstations is protected by bitlocker encryption. Encryption is forced on workstations through AD.

Removable storage devices are recommended to secure with bitlocker encryption if they contain confidential information. The user manages the encryption keys by creating a password for the storage device.

PERSONAL DATA LIFECYCLE PROCESS

iLOQ's personal data lifecycle has been described Personal data lifecycle

PRIVACY POLICY, INTERNAL

iLOQ Oy's Policy for Data Handling

PERSONAL DATA ACT (523/1999) 10 § AND 24 § & GDPR (679/2016) ARTICLES 13, 14 AND 30

1) CONTROLLER

Name: iLOQ Oy
Business ID: 1842821-6
Address: Elektroniikkatie 10, 90590 Oulu

In this Privacy Policy the controller may also be referred to as "we".

2) PERSON IN CHARGE

Name: Jaana Klinga
Phone: +358 44 435 2403
Email: jaana.klinga@iloq.com

3) THE CATEGORIES OF DATA SUBJECTS

iLOQ Oy's Privacy Policy concerns the following categories of data subjects:

3.1) persons who contact iLOQ Oy via email, through the web pages or the sales department.
3.2) persons who are employed by iLOQ Oy or seek employment from iLOQ Oy.
3.3) persons who visit iLOQ Oy's premises.

In this Privacy Policy data subjects may also be referred to as "person", "them" or "you".

4) THE CATEGORIES OF PERSONAL DATA

The data files concerning the data subjects of Sections 3.1) – 3.3) may contain the following categories of personal data:

- contact information, such as full name, job title, address, phone numbers and e-mail addresses;
- security camera footage;
- other information gathered with the data subject's consent.

The data files concerning the data subjects of Section 3.1) may also contain the following categories of personal data:

- data about your device, such as information about the device you use: type of your device, your IP-address and various diagnostic data;

- user information, such as username, password and other unique identification browsing, search information and other information concerning your use of our services;
- information regarding the customer relationship, such as billing and payment information, product-, service- and ordering information, information regarding customer feedback, contacts and cancellation.

The data files concerning the data subjects of Section 3.2) may also contain the following categories of personal data:

- personal identification numbers and username
- nationality, age, gender, title or profession and mother tongue;
- work background, CV, application letter and photo;
- data concerning payroll;
- union affiliation and data concerning employee health;
- security clearance;
- personality and aptitude test results;
- work hours monitoring, annual vacation information and travel expenses.

5) PURPOSE OF THE PROCESSING OF PERSONAL DATA

Personal data of the data subjects of Sections 3.1) – 3.3) can be handled for following purposes:

- analysis and statistics;
- customer service;
- exchanging contact information with the consent of the data subject;
- for improving our user experience;
- property surveillance;
- marketing;
- operative procedures;
- to enable us to comply with our legal and regulatory obligations.

Personal data of the data subjects of Section 3.1) can also be handled for following purposes:

- management and development of the customer relationship;
- marketing, market surveys and studies.

Personal data of the data subjects of Section 3.2) can also be handled for following purposes:

- management and development of the employee and jobseeker relationships;
- management of employment contracts;
- upholding a training register;
- upholding holiday and bonus lists;
- payroll and benefit management;

- property access management;
- recruitment process;
- improving well-being at work;
- internal address books;
- other employer responsibilities.

Personal data of the data subjects of Section 3.3) can also be handled for following purposes:

- upholding a training register;
- meeting notes and memos;
- calendar records.

Personal data can also be processed by iLOQ Oy's affiliate companies, if any, in accordance with the Finnish Personal Data Act, the GDPR and the Finnish Data Protection Act.

6) LEGAL BASIS FOR PROCESSING

The controller has the right to process the personal data of the data subjects based on the:

- consent received from the data subjects;
- performance of a contract in which the data subject acts as the contact person of the organizer;
- legal obligation to which the controller is subject.

7) REGULAR SOURCES OF INFORMATION

Information regarding the data subjects are regularly gathered:

- from data subjects themselves via phone, internet, e-mail or in other similar fashion;
- with cookies and other similar tech;
- CVs;
- iLOQ Oy's recruitment partner;
- employment contracts;
- occupational healthcare;
- security cameras and key logs.

Personal data concerning data subjects is transferred from third parties in accordance with the Finnish Personal Data Act and the GDPR.

8) PERIOD FOR WHICH THE PERSONAL DATA WILL BE STORED

The controller shall not store the personal data longer than is necessary, taking into consideration the purpose for the processing of personal data. Upon request, all data on a data subject will be removed immediately (see section 11 for details).

- Customer and contact person data will be stored until they are **no longer useful,** or the data subject **asks for its removal**.
- CV's, copies of employment certificates and the recruitment evaluation of the person chosen for the job are stored for the **duration of the person's employment contract**, after which they are destroyed.
- Drug test records are stored for the **duration of the person's employment contract**, after which it will be destroyed.
- Data on job applicants is **not stored without their consent**. With their consent the data will be stored for **6 months**, after which it will be destroyed.
- Data on job applicants who are not selected for the job they applied to are **not stored without their consent**. With their consent the data will be stored for **6 months**, after which it will be destroyed.
- Access logs from the keys will be stored for the **duration of the person's employment contract**, after which they are destroyed.
- Payroll details will be stored for **10 years after the last salary period** in accordance to the Accounting Act (1336/1997).
- Details required for an employment certificate will be stored for **10 years after the end of the employment contract** in accordance to the Employment Contracts Act (55/2001).
- Security camera footage will be stored for **90 days after the capture of the footage**.

The controller inspects the necessity of the personal data stored on a monthly basis.

9) CATEGORIES OF RECIPIENTS OF PERSONAL DATA

The recipients of personal data may consist of the following categories:

- iLOQ Oy's affiliate companies;
- third parties who offer cloud services;
- third parties who offer accounting, marketing and auditing services;
- third parties who offer occupational healthcare and benefits services
- third parties who help iLOQ Oy to fulfill its legal obligations;

Email addresses concerning data subjects may be disclosed with the data subject's consent for marketing purposes in accordance with the Finnish Personal Data Act and the GDPR.

Contact information concerning data subjects may be disclosed with the data subject's consent to third parties in accordance with the Finnish Personal Data Act and the GDPR.

10) REGULAR DISCLOSURE OF DATA AND INFORMATION TRANSFER OUTSIDE OF EU OR THE EUROPEAN ECONOMIC AREA

Information may be transferred and stored to a server outside of EU or the European Economic Area to be processed by the Controller or Controller's affiliate on Controller's behalf in accordance with the Finnish Personal Data Act, the GDPR and the Finnish Data Protection Act.

11) DATA SUBJECTS' RIGHTS

The data subject has a right to use all of the below mentioned rights.

The contacts concerning the rights shall be submitted to the person in charge of the data file stated in Section 2. The rights of the data subject can be put into action only when the data subject has been satisfactorily identified.

Right to inspect

Having presented the adequate and necessary information, the data subject has the right to know what, if any, data the controller has stored of her/him into this register. While providing the requested information to the data subject, the controller must also inform the data subject of the register's regular sources of information, to what are the personal data used for and where is it regularly disclosed to.

Right to rectify and erasure

The data subject has a right to request the controller to rectify the inaccurate and incomplete personal data concerning the data subject.

The data subject can request the controller to erase the personal data concerning the data subject, if:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws consent on which the processing is based on;
- the personal data has been unlawfully processed; or
- the personal data has to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject to.

If the controller does not accept the data subject's request to rectify or erase the personal data, it must give a decision of the matter to the data subject in a written form. The decision must include the reasons for which the request was not granted. The data subject may then refer the matter to the relevant authorities (Data Protection Ombudsman).

The controller must inform the party to whom the controller has disclosed the personal data to or has received the personal data from of the rectification or erasure of personal data. However, there is no such obligation where the fulfilment of the obligation would be practically impossible or otherwise unreasonable.

Right to restriction of processing

The data subject can request the controller to restrict the processing of the personal data concerning the data subject where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
- the controller no longer needs the personal data for the purposes of the processing, but the personal data is required by the data subject for the establishment, exercise or defense of legal claims.

If the controller has based the restriction of the processing of personal data on the abovementioned criteria, the controller shall give a notification to the data subject before removing the restriction.

Right to object

Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning her/him for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Right to data portability

The data subject shall have the right to receive the personal data concerning her/him, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data has been provided.

Right to withdraw consent

Where the legal basis for the processing of personal data is the consent of the data subject, the data subject shall have the right to withdraw their consent.

12) RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

The data subject shall have the right to lodge a complaint with a supervisory authority, if the data subject considers that the processing of personal data relating to the person infringes the GDPR. The complaint can be lodged in the Member State of the persons habitual residence, place of work or place of the alleged infringement.

13) MERGERS AND ACQUISITIONS

Regarding mergers, acquisitions or divestiture of all parts of Company iLOQ Oy's business, the acquiring entity, as well as its business partners will obtain access to data managed by iLOQ Oy, and this may include personal data. In the aforementioned case, such external parties will enter into a non-disclosure agreement with iLOQ Oy, which covers the potential disclosure of personal data.

14) DATA PROTECTION PRINCIPLES

iLOQ Oy uses all reasonable efforts to maintain physical, electronic, and administrative safeguards to protect personal information from unauthorized or inappropriate access, but iLOQ Oy notes that the Internet is not always a secure medium. iLOQ Oy restricts access to information about data subjects only to the personnel of iLOQ Oy that need to know the information e.g. for responding to inquiries or requests made by the data subjects. The employees of iLOQ Oy follow the iLOQ IT-Management and Information Security Guidelines (ID:16061) to assure that both confidential customer information and iLOQ's own operational data are kept safe. This minimizes the potential risks and threats of iLOQ's business activities.

Data handling and transfer are protected by usernames, passwords, firewalls and other administrative data security measures. Access to rooms with physical archives are restricted with coded keys and the management of their access rights. Use of the access management system is restricted with a username and password as well as a physical master key, the iButton. Access to the digital folder management system is restricted with editing and viewing rights. Fujitsu Services Oy is responsible for the management of the access logs of the keys and they operate in accordance to the ISO:27001 information security management standard and using secured datalinks.

PRIVACY POLICY, EXTERNAL

iLOQ Oy's PRIVACY POLICY

PERSONAL DATA ACT (523/1999) 10 § AND 24 § & GDPR (679/2016) ARTICLES 13, 14 AND 30

1) CONTROLLER
Name: iLOQ Oy
Business ID: 1842821-6
Address: Elektroniikkatie 10, 90590 OULU

In this Privacy Policy the controller may also be referred to as "we".

2) PERSON IN CHARGE
Name: Jaana Klinga
Phone: +358 44 435 2403
Email: jaana.klinga@iloq.com

3) THE CATEGORIES OF DATA SUBJECTS
iLOQ Oy's Privacy Policy concerns the following categories of data subjects:

3.4) persons who contact iLOQ Oy via email or through the service:
3.5) persons who belong to iLOQ Oy's customer, supplier or partner registers;
3.6) persons seek employment from iLOQ Oy.

In this Privacy Policy data subjects may also be referred to as "you" and "them".

4) THE CATEGORIES OF PERSONAL DATA
The data files concerning the data subjects of Sections 3.1) – 3.3) may contain the following categories of personal data:

- contact information, such as full name, address, phone numbers and e-mail addresses;
- possible other information gathered with the data subject's consent.

The data files concerning the data subjects of Section 3.1) may also contain the following categories of personal data:

- data about your device, such as information about the device you use: type of your device, your IP-address and various diagnostic data;

- user information, such as username, password and other unique identification browsing, search information and other information concerning your use of our services.

The data files concerning the data subjects of Section 3.2) may also contain the following categories of personal data:

- information regarding the customer relationship, such as billing and payment information, product-, service- and ordering information, information regarding customer feedback, contacts and cancellation.

The data files concerning the data subjects of Section 3.3) may also contain the following categories of personal data:

- nationality, age, gender, title or profession and mother tongue;
- work background and photo.

5) PURPOSE OF THE PROCESSING OF PERSONAL DATA

Personal data of the data subjects of Sections 3.1) – 3.3) can be handled for following purposes:

- customer service;
- improving our user experience;
- analysis and statistics;
- to enable us to comply with our legal and regulatory obligations.

Personal data of the data subjects of Section 3.1) can also be handled for following purposes:

- management and development of the customer relationship;
- marketing, market surveys and studies.

Personal data of the data subjects of Section 3.2) can also be handled for following purposes:

- exchanging contact information with the consent of the data subject

Personal data of the data subjects of Section 3.3) can also be handled for following purposes:

- management and development of the jobseeker relationships

Personal data can also be processed by iLOQ Oy's Finnish affiliate companies, if any, in accordance with the Finnish Personal Data Act, the GDPR and the Finnish Data Protection Act.

6) LEGAL BASIS FOR PROCESSING

The controller has the right to process the personal data of the data subjects based on the:

- consent received from the data subjects;
- performance of a contract in which the data subject acts as the contact person of the organizer;

- legal obligation to which the controller is subject.

7) REGULAR SOURCES OF INFORMATION

Information regarding the data subjects are regularly gathered:

- from data subjects themselves via phone, internet, e-mail or in other similar fashion;
- with cookies and other similar tech;
- CVs and application letters;
- referrals.

8) PERIOD FOR WHICH THE PERSONAL DATA WILL BE STORED

The controller shall not store the personal data longer than is necessary, taking into consideration the purpose for the processing of personal data.

- Customer and contact person data will be stored until they are **no longer useful** or the data subject **asks for its removal**.
- Data on job applicants **is not stored without their consent**. With their consent the data will be stored for **6 months**, after which it will be destroyed.

The controller inspects the necessity of the personal data stored on a monthly basis.

9) CATEGORIES OF RECIPIENTS OF PERSONAL DATA

The recipients of personal data may consist of the following categories:

- iLOQ Oy's affiliate companies;
- third parties who offer cloud services;
- third parties who offer accounting, recruiting, marketing and auditing services;
- third parties who help iLOQ Oy to fulfill its legal obligations.

Information concerning data subjects may be disclosed with the data subject's consent for marketing purposes in accordance with the Finnish Personal Data Act and the GDPR.

Contact information concerning data subjects may be disclosed with the data subject's consent to third parties in accordance with the Finnish Personal Data Act and the GDPR.

10) REGULAR DISCLOSURE OF DATA AND INFORMATION TRANSFER OUTSIDE OF EU OR THE EUROPEAN ECONOMIC AREA

Information may be transferred and stored to a server outside of EU or the European Economic Area to be processed by the Controller or Controller's affiliate on Controller's behalf in accordance with the Finnish Personal Data Act, the GDPR and the Finnish Data Protection Act.

11) DATA SUBJECTS' RIGHTS

The data subject has a right to use all of the below mentioned rights.

The contacts concerning the rights shall be submitted to the person in charge of the data file stated in Section 2. The rights of the data subject can be put into action only when the data subject has been satisfactorily identified.

Right to inspect

Having presented the adequate and necessary information, the data subject has the right to know what, if any, data the controller has stored of her/him into this register. While providing the requested information to the data subject, the controller must also inform the data subject of the register's regular sources of information, to what are the personal data used for and where is it regularly disclosed to.

Right to rectify and erasure

The data subject has a right to request the controller to rectify the inaccurate and incomplete personal data concerning the data subject.

The data subject can request the controller to erase the personal data concerning the data subject, if:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws consent on which the processing is based on;
- the personal data has been unlawfully processed; or
- the personal data has to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject to.

If the controller does not accept the data subject's request to rectify or erase the personal data, it must give a decision of the matter to the data subject in a written form. The decision must include the reasons for which the request was not granted. The data subject may then refer the matter to the relevant authorities (Data Protection Ombudsman).

The controller must inform the party to whom the controller has disclosed the personal data to or has received the personal data from of the rectification or erasure of personal data. However, there is no such obligation where the fulfilment of the obligation would be practically impossible or otherwise unreasonable.

Right to restriction of processing

The data subject can request the controller to restrict the processing of the personal data concerning the data subject where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or
- the controller no longer needs the personal data for the purposes of the processing, but the personal data is required by the data subject for the establishment, exercise or defense of legal claims.

If the controller has based the restriction of the processing of personal data on the abovementioned criteria, the controller shall give a notification to the data subject before removing the restriction.

Right to object

Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning her/him for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Right to data portability

The data subject shall have the right to receive the personal data concerning her/him, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data has been provided.

Right to withdraw consent

Where the legal basis for the processing of personal data is the consent of the data subject, the data subject shall have the right to withdraw her/his consent.

12) RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY

The data subject shall have the right to lodge a complaint with a supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes the GDPR. The complaint can be lodged in the Member State of her/his habitual residence, place of work or place of the alleged infringement.

13) MERGERS AND ACQUISITIONS

In connection with mergers, acquisitions or divestiture of all parts of iLOQ Oy's business, the acquiring entity, as well as its business partners will obtain access to data managed by iLOQ Oy, and this may include personal data. In the aforementioned case, such external parties will enter into a non-disclosure agreement with iLOQ Oy, which covers the potential disclosure of personal data.

14) DATA PROTECTION PRINCIPLES

iLOQ Oy uses all reasonable efforts to maintain physical, electronic, and administrative safeguards to protect personal information from unauthorized or inappropriate access, but iLOQ Oy notes that the Internet is not always a secure medium. iLOQ Oy restricts access to information about data subjects only to the personnel of iLOQ Oy that need to know the information e.g. for responding to inquiries or requests made by the data subjects.

CHANGE HISTORY

Revision	Date (YYYY-MM-DD)	Author	Change Reason
0.1	2022-10-12	H. Leskinen	First draft (policies for the same documents)
1.0	2022-10-12	H. Leskinen	For approval (by T. Ainali)
1.1	2023-03-03	H. Leskinen	Person in charge changed
2.0	2023-03-03	H. Leskinen	For approval (by T. Ainali)
2.1	2023-11-23	T. Ainali, M-K Kuoppala, H. Ahola, J. Koivula, T. Lappi, T. Karhu, H. Leskinen	Introduction chapter added, policies updated and reviewed
2.2	2023-12-01	T. Ainali, M-K Kuoppala, H. Ahola, J. Koivula, T. Lappi, T. Karhu, H. Leskinen	Policies updated and reviewed
2.3	2023-12-12	Leadership Team E. Sankari, V. Tolvanen, H. Hiltunen, J. Klinga, J. Lampinen, M. Tuomikoski, T. Thörewik, T. Ainali, T. Pirskanen, T. Karjalainen	Reviewed by Leadership Team

Revision	Date (YYYY-MM-DD)	Author	Change Reason
3.0	2023-12-12	Leadership Team E. Sankari, V. Tolvanen, H. Hiltunen, J. Klinga, J. Lampinen, M. Tuomikoski, T. Thörewik, T. Ainali, T. Pirskanen, T. Karjalainen	Approved by Leadership Team
3.1	2024-03-28	H. Ahola, MK Kuoppala, J. Koivula, H. Leskinen	Policy reviewed from cyber security point of view. Cyber security added to headline.
3.2	2024-09-26	H. Leskinen	Std and objective references added to information security policy
4.0	2024-11-11	Leadership Team	Reviewed and approved to the presented to the Finance and Audit Committee and thereafter to the Board for approval.
5.0	4th December 2024	Leadership Team	Reviewed and Approved