INTERNAL

PRIVACY POLICY

VERSION: 1.2
DATE: 27.09.2023

work smarter

KJAER DATA | Hollufgårds Allé 1 | 5220 Odense SØ
P: +45 63 10 12 00 | E: mail@kjaer-data.com | www.kjaer-data.com

Table of Content

1.0 Introduction

This privacy policy is developed to ensure that KJAER DATA complies with relevant laws and guidelines regarding the protection of personal data. We are committed to safeguarding the personal information and confidentiality of personal information collected and processed during our business operations.
This policy outlines the principles and responsibilities that all employees must follow to ensure the protection and proper handling of personal data.

2.0 Scope

This policy applies to all employees, contractors, and third parties acting on behalf of KJAER DATA who have access to personal information. It covers all personal data collected, processed, or stored by KJAER DATA.

3.0 Responsibilities

3.1 HR and Cybersecurity as GDPR Responsibles

An appointed person in HR- and one in the Cybersecurity department are responsible for implementing this policy overseeing and ensuring compliance with data protection law, and all employees are responsible for compliance.

HR/ Mette Nyland Kjær: mnk@kjaer-data.com
Cybersecurity department: Claus Jacobsen: cja@kjaer-data.com

Responsibility means that responsible persons mentioned above ensure that data is deleted, and that data has been deleted in accordance with internal procedures and related laws.

3.2 All Employees

- All employees must familiarize themselves with this policy and comply with its provisions.
- All employees must fill in a GDPR/dataetics questionnaire concerning:
  - What data is collected (personal data / sensitive data)
  - Where is data stored
  - Who has access
  - What is the purpose (employment contracts, bank information, customer handling (see relevant policy) ect.)
  - When will it be deleted etc.

HR/Cybersecurity is sender and this half yearly process is to ensure right handling of personal data. This process and collected data will be reviewed yearly.

- Employees must only access personal data/sensitive data when it is necessary for their job

responsibilities.

- Employees should report any data breaches, unauthorized access, or potential privacy violations to mnk@kjaer-data.com
- Employees must participate in our data protection training and awareness programs as required by the company. See above.

4.0 Implementation

Implementation includes data collection, storage, access controls, and regular audits.

5.0 Collection and Use of Personal Data/ Sensitive Data

- KJAER DATA will collect and use personal data/Sensitive Data only for legitimate business purposes, and employees should obtain appropriate consent when required.
- Personal data/Sensitive data is collected and processed accurately and lawfully.
- Employees should minimize the amount of personal data they collect and use it only for the intended purpose.
- Employees who receive personal and sensitive information, for which she/he has no purpose, must delete it immediately (shift/delete) and refer to HR.

6.0 Data Security

- All employees must ensure the security and confidentiality of personal and sensitive data. This includes protecting data from unauthorized access, disclosure, alteration, or destruction. To handle this every employee must document their handling of all personal data, a process initiated by HR / cybersecurity department via forms/templates to be reviewed on a regular basis. See 3.2.
- Access to personal and sensitive data should be limited to employees with a legitimate need to know.
- Personal and sensitive data should be stored securely, and physical and electronic safeguards should be in place.

7.0 Data Retention

- Personal and sensitive data should only be retained for the period necessary to fulfill the purpose for which it was collected. KJAER DATA follow the respective regulations/laws.
- Employees must follow our data retention and disposal policies.

8.0 Reporting Data Breaches

- Any actual or suspected data breaches must be reported immediately to the mnk@kjaer-data.com.

9.0 Training and Awareness

KJAER DATA will provide regular training and awareness programs to educate employees on data protection policies and procedures. See 3.2 and 6.0.

10.0 Processing of Personal Data about Job Applicants

KJAER DATA receives applications and CVs through a secure database via our website. HR, CEO and one appointed IT have access. HR process the personal and sensitive information which is handled in accordance with relevant data protection regulations.

10.1 Storage of Personal Data about Applicants

KJAER DATA retains personal information about applicants in accordance with relevant laws and guidelines regarding to GDPR. In this case, personal and sensitive information of this sort will be stored securely up to 6 months unless a consent on prolonging the time has been given from the candidate.

11.0 Right to Access and Rectify

KJAER DATA provides our employees with the right to access and obtain a copy of the personal information we hold about them. We ensure that employees can correct any inaccurate information.

12.0 Right to Erasure and Restriction of Processing

KJAER DATA grants our employees the right to request the erasure or restriction of the processing of their personal data in accordance with relevant laws and guidelines regarding to GDPR.

13.0 Right to Object

KJAER DATA acknowledges our employees' right to object to the processing of their personal data in certain situations and will adhere to this right in accordance with relevant laws and guidelines regarding to GDPR.

14.0 Disclosure of Personal Data

KJAER DATA does not disclose employees' personal data to third parties unless necessary to fulfil work-related purposes or in accordance with relevant laws and guidelines regarding to GDPR.

15.0 Storage of Information about Departed Employees

KJAER DATA deletes or anonymizes personal information about departed employees when it is no longer necessary to retain them in accordance with relevant laws and guidelines regarding to GDPR.
In this case, personal information of this sort will be stored securely up to 5 years.

16.0 Control Measures for Remote Work

KJAER DATA has not implemented additional control measures for remote work unless required in accordance with relevant laws and regulations.

17.0 Contact Information

If you have questions or concerns regarding our processing of personal data or this privacy policy, please contact us at the following address: mnk@kjaer-data.com

18.0 Review and updates including reporting to Management

- This internal privacy policy will be reviewed regularly to ensure compliance with changing data protection regulations and business needs.
- Updates to the policy will be communicated to all employees.
- Regular audits and reporting to the management board ensure ongoing compliance with this policy.

19.0 Compliance with Laws

KJAER DATA is committed to complying with all applicable data protection laws and regulations.

20.0 Approved

This policy is approved and signed by KJAER DATAs CEO on September 21, 2023.

21.0 Owner information

KJAER DATA
Hollufgårds Allé 1
5220 Odense SØ
+45 63 10 12 00
Mail@kjaer-data.com
CVR: 30836030

Last updated: 27/09 2023

CEO
Henrik Nyland Kjær