DEK Technologies Personal Data Policy

Abstract

This document describes the personal data policy at DEK Technologies

Contents

1 INTRODUCTION

This document provides guidelines on how to manage personal data in accordance with the European Union (EU) General Data Protection Regulation (GDPR) for DEK Technologies (DEK Corporation Pty Ltd [Australia], DEK Technologies Sweden AB [Sweden], DEK Technologies Vietnam Co LTD [Vietnam], and DEK Italia SRL [Italy]), hereafter referred to as the Company or as DEK.

1.1 HOW TO USE THIS POLICY

This policy is a high-level document that describes what and why personal data that is stored by the Company.

In addition, all DEK entities must also fulfill local government regulations regarding data privacy and handling of personal data.

2 GENERAL PRINCIPLE OF PERSONAL DATA

The Company shall not store or manage any personal data (see Chapter 9.1 PERSONAL DATA for definition) in any form (digital or physical) without one of the following conditions being meet:

- Prior written consent from the individual whom the Company is storing data of, defined in Chapter 3 CONSENT, or;
- If storage or management of personal data of an individual is necessary to fulfill some specific purpose for the Company, defined in Chapter 4 COMPANY SPECIFIC PURPOSES TO STORE PERSONAL DATA.
- Prior written consent and authorisation from any customers of the Company, where the customer requires the Company to process Personal Data on its behalf.

All Personal Data must only be used to satisfy contractual obligations for the Company or customers of the Company and for no other purpose.

All Personal Data must only be stored, printed or copied for purpose of use only. Redundant storage, printing or copying of such data is STRICTLY prohibited.

3 CONSENT

This chapter defines how a consent is given by a natural person to the Company and how the Company manages, stores and destroys the consent.

3.1 DEFINITION OF A CONSENT

A consent shall always:

- Be given on a voluntary basis and;
- It is specific, for what purpose and period is the consent given and;
- It is unambiguously and;
- Individually and;
- In writing in two copies signed by the natural person giving consent and a representative of the Company and;
- A separate document from all other documents and/or agreements and;
- All consents can at any time be recalled by the natural person.

3.2 MANAGEMENT AND STORAGE OF A CONSENT

The Company shall store all consents in a safe and controlled way which allows only authorized personnel from the Company to access all consents.

The authorized personnel that are allowed to access consents are part of the Management Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

3.3 DESTRUCTION OF A CONSENT

The Company will destroy a consent 5 years after the consent has ceased to be valid, either by definition or by recall.

4 COMPANY SPECIFIC PURPOSES TO STORE PERSONAL DATA

To be able to perform the services and duties that are obliged and expected by the Company's customers, employees, suppliers, regulations and laws, the Company stores, manages and destroys personal data according to this Chapter.

4.1 HUMAN RESOURCE (HR)

The Human Resource function of the Company manages and stores data of the employees of the Company in the following way:

4.1.1 Employment Contract

4.1.1.1 Data that is stored

The employment contract contains the following personal data of the employee:

- Full Name;
- Social Identity Number and date of birth;
- Salary, Occupational Pension and other Benefits;
- Home address;
- Bank account details;
- Optional: 1 or 2 name(s) with phone numbers to close relatives

4.1.1.2 Management and storage

The Company stores all employee contracts on both paper and in digital format.

4.1.1.3 Access

The authorized personnel that are allowed to access are part of the HR Group of the Company or Finance Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.1.1.4 Destruction

The employment contract is destroyed 10 years after the last day of employment.

4.1.1.5 Thinning

Once per year the employment contracts are thinned.

4.1.1.6 Usage

The Company uses the data in the employment contract for the following purposes:

- Secure identity of an individual;
- Pay salaries;
- In the case concerned pay occupational pension;
- In the case concerned register for occupational group life insurance and labor market no-fault liability insurance;
- Social-Health-Unemployment insurance registration/cancellation
- Extra insurance registration/cancellation
- Pay taxes to tax authorities;
- Create a digital corporate identity for the Company;
- Create a mail address;
- In the case concerned register a phone and/or mobile phone with associated phone number;
- In the case concerned register a laptop;
- In case of an accident contact relatives.

4.1.2 CV

4.1.2.1 Data that is stored

The CV contains the following personal data of the employee:

- Full Name;
- Social Identity Number and date of birth;
- Picture of the individual;
- Education and work-related experiences;
- Competencies and qualifications.

4.1.2.2 Management and storage

The Company stores all CVs on both paper and in digital format.

4.1.2.3 Access

The authorized personnel that are allowed to access are part of the Basic Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.1.2.4 Destruction

The CV is destroyed 2 years after the last day of employment.

4.1.2.5 Thinning

Once per year the CVs are thinned.

4.1.2.6 Usage

The Company uses the data in the CV for the following purposes:

- To be able to promote and sell the competence of the Company

4.1.3 Recruitment

4.1.3.1 Data that is stored

The recruitment tool contains the following personal data of a potential employee, hereafter the Candidate:

- Full Name;
- Digital identity, mail;
- Phone number;
- Picture of the individual;
- Education and work-related experiences;
- Competencies and qualifications.

4.1.3.2 Management and storage

The Company stores all candidate data on both paper and in digital format. The personal data of the Candidate is stored for maximum 12 months, then the Candidate either revokes or consent that the Company continues to store the personal data for another 12 months.

4.1.3.3 Access

The authorized personnel that are allowed to access are part of the HR Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.1.3.4 Destruction

The Candidate can themselves decide how long the personal data should be stored and can at any time decide to order destruction of the personal data.

4.1.3.5 Thinning

Done on a rolling basis.

4.1.3.6 Usage

The Company uses the data from the Candidate for the following purposes:

- To be able to recruit new employees for the Company

4.1.4 Time Reporting

4.1.4.1 Data that is stored

The time reporting tool contains the following personal data of an employee:

- Full Name;
- Digital identity, mail;
- Attendance, Vacation, Time-off in Lieu, Personal Leave, Sick Leave, Parental Leave and Take Care of Kids Leave.

4.1.4.2 Management and storage

The Company stores all time reporting on both paper and in digital format.

4.1.4.3 Access

The authorized personnel that are allowed to access are part of the HR Group of the Company and the Finance Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.1.4.4 Destruction

The time reporting data is destroyed 10 years after the last day of employment.

4.1.4.5 Thinning

Once per year the time reporting is thinned.

4.1.4.6 Usage

The Company uses the data in the time reporting tool for the following purposes:

- To be able to pay correct salaries;
- To be able to report to applicable authorities for Parental Leave, Sick Leave and Take Care of Kids Leave;
- To be able to keep track of Sick Leave in accordance with the law.

4.2 FINANCE

The Finance function of the Company manages and stores data of the employees of the Company in the following way:

4.2.1 Accounting and Financial Data

4.2.1.1 Data that is stored

The accounting and financial data contains the following personal data of the employee:

- Full Name;
- Social Identity Number and date of birth;
- Salary, Occupational Pension and other Benefits;
- Home address;
- Bank account details.

4.2.1.2 Management and storage

The Company stores all accounting and financial data on both paper and in digital format.

4.2.1.3 Access

The authorized personnel that are allowed to access are part of the Finance Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.2.1.4 Destruction

The accounting and financial data is destroyed after 10 years.

4.2.1.5 Thinning

Once per year the financial data is thinned.

4.2.1.6 Usage

The Company uses the accounting and financial data in the following purposes:

- Pay salaries;
- In the case concerned pay occupational pension;
- In the case concerned register for occupational group life insurance and labor market no-fault liability insurance;
- Pay taxes to tax authorities;
- Accounting and financial reporting in accordance with the law.

4.3 SALES AND MARKETING

4.3.1 Customer Relationship Management (CRM) Tool

4.3.1.1 Data that is stored

The CRM Tool contains the following personal data, hereafter the Customer:

- Full Name;
- Digital Identity, mail;
- Work related role;
- Employer.

4.3.1.2 Management and storage

The Company stores all CRM Tool data on both paper and in digital format.

4.3.1.3 Access

The authorized personnel that are allowed to access are part of the BD Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.3.1.4 Destruction

The CRM Tool data is destroyed after 2 years of the last interaction with the Customer.

4.3.1.5 Thinning

Once per year the CRM Tool data is thinned.

4.3.1.6 Usage

The Company uses the CRM Tool data for the following purposes:

- Keep contact with the current Customers;
- Keep contact with future potential Customers.

4.4 OPERATIONAL

4.4.1 Digital Identity

4.4.1.1 Data that is stored

The digital identity contains the following personal data of the employee:

- Full Name;
- Date of birth;
- Picture of the individual.

4.4.1.2 Management and storage

The Company stores digital identities on both paper and in digital format.

4.4.1.3 Access

The authorized personnel that are allowed to access are part of the Basic Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.4.1.4 Destruction

The digital identity is destroyed 2 months after the last day of employment.

4.4.1.5 Thinning

Done on a rolling basis.

4.4.1.6 Usage

The Company uses the data in the digital identity for the following purposes:

- To be able to communicate internally and externally

4.4.2 Internal presentation

4.4.2.1 Data that is stored

The internal presentation contains the following personal data of the employee:

- Full Name;
- Picture of the individual;
- Education and work-related experiences;
- Competencies and qualifications.

4.4.2.2 Management and storage

The Company stores internal presentation on both paper and in digital format.

4.4.2.3 Access

The authorized personnel that are allowed to access are part of the Basic Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.4.2.4 Destruction

The internal presentation is destroyed 5 years after the last time it was used.

4.4.2.5 Thinning

Once per year the internal presentations are thinned.

4.4.2.6 Usage

The Company uses the data in the internal presentations for the following purposes:

- To be able to present ongoing activates in the Company

4.4.3 External presentations

4.4.3.1 Data that is stored

The external presentation contains the following personal data of the employee:

- Full Name;
- Picture of the individual;
- Education and work-related experiences;
- Competencies and qualifications.

4.4.3.2 Management and storage

The Company stores external presentation on both paper and in digital format.

4.4.3.3 Access

The authorized personnel that are allowed to access are part of the Basic Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

4.4.3.4 Destruction

The internal presentation is destroyed 5 years after the last time it was used.

4.4.3.5 Thinning

Once per year the external presentations are thinned.

4.4.3.6 Usage

The Company uses the data in the external presentations for the following purposes:

- To be able to present ongoing activates in the Company;
- To be able to promote and sell the competence of the Company.

5 ACCESS TO OWN PERSONAL DATA

All personal data that is managed by the Company can be accessed by the single individual by putting forward a request for access to own personal data.

5.1 REQUEST FOR ACCESS TO OWN PERSONAL DATA

To get access to the data about yourself that the Company has stored about you:

- The request must be in writing on a paper;
- The individual must provide a valid identification;
- Where personal data is processed on behalf of customers of the Company, written authorization from the individual and the Company's customer must be obtained.
- The request must be put forward to the General Management Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

5.2 RECEIVING OWN PERSONAL DATA

Once a valid Request for access to own personal data has been put forward to the Company:

- The Company will within 2 months return a digital copy of all data that the Company stores about the individual;
- The digital copy will only be handed out to the single individual that made the request.

5.3 CORRECTION/UPDATE OF PERSONAL DATA

In the event that personal data is stored incorrectly or is required to be updated, a request for such actions must be put forward to the Company:

- The request must be in writing on a paper;
- The individual must provide a valid identification;
- Where personal data is processed on behalf of customers of the Company, written authorization from the individual and the Company's customer must be obtained.
- In the event that the correctness of personal data is disputed, all processing associated with the personal data must be halted until an agreed action is reached.
- The request must be put forward to the General Management Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

6 TRANSFERING OF PERSONAL DATA TO ANOTHER ORGANIZATION OUTSIDE OF THE COMPANY

In the case that the Company needs to transfer personal data to a Government organization, authorities or other companies or organizations to fulfill laws, regulations or in the interest of the individual whose personal data will be transferred.

The Company will inform the individual in the following way:

- What personal data is transferred;
- Where the personal data is transferred;
- For what purpose is the personal data transferred.

In the event the Company's customers personal data is requested to be transferred, the customer will be given prior notice before any action is taken.

7 THE RIGHT TO BE FORGOTTEN

An individual has the right to be forgotten, this means that the Company will delete all personal data of the single individual that is not required by the Company due to laws or regulations to keep.

7.1 REQUEST FOR DELETION OF OWN PERSONAL DATA

To be forgotten by the Company, a request has to be put forward:

- The request must be in writing on a paper;
- The individual must provide a valid identification;
- The request must be put forward to the General Management Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

8 INCIDENT HANDLING

In case of a breach, leak or personal data coming into the public or wrong possession.

The Company will:

- Immediately stop the ongoing leak or breach;
- Immediately inform responsible authorities and/or relevant customers;
- Inform the individual of what personal data that has leaked and to whom/where it has leaked;

Any employee of DEK who discovers a breach must immediately notify any one of the General Management Group of the Company, see Chapter 9.2 AUTHORIZED PERSONNEL OF THE COMPANY.

9 DEFINITIONS

9.1 PERSONAL DATA

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- A name;
- An identification number;
- Location data;
- An online identifier or;
- To one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

9.2 AUTHORIZED PERSONNEL OF THE COMPANY

All personnel employed by the Company belong to one or more group(s) that have different levels of authority.

9.2.1 Basic Group

All employees of the Company belong to the Basic Group.

9.2.2 HR Group

Employees employed within the Human Resource function of the Company belong to the HR Group.

9.2.3 Finance Group

Employees employed within the finance function of the Company belong to the Finance Group.

9.2.4 BD Group

Employees employed within the Business Development function of the Company belong to the BD Group.

9.2.5 Management Group

Employees employed with a managerial function of the Company belong to the Management Group.

9.2.6 General Management Group

Employees employed as General Manager, Managing Director, Chief Executive Officer and Chief Operational Officer functions of the Company belong to the General Management Group.

10 REVIEW TIMEPLAN

This document will undergo a review every 12 months or whenever there are significant changes to relevant government policies, customer polices or company policies.

11 REVISION HISTORY

Rev A	2018-05-23	First version of the document.
Rev B	2019-03-21	Updated policies.
Rev C	2019-07-21	Updated spelling and English errors.