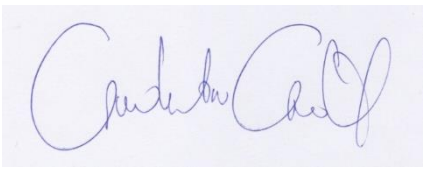
Privacy and Data Processing Policy and Records of Mimox Kft.

Budapest, September 2, 2020

Version 4.0

Approved by



Csudinka Csudutov
Managing Director

Table of Contents

I Objective

The objective of this Privacy and Data Protection Policy ("Policy") is to ensure the data protection rights applicable to personal data in relation to the activities of Mimox Kft. ("Company" or "Organization"), prevent the unauthorized use of personal data, and determine the data protection and safety measures that control the processing of personal data.

Any personal data may be processed by the Company for specified purposes or exercising rights or fulfilling requirements only. The purpose of processing, which is defined for the individual occurrences of processing, shall be valid and available throughout the duration of processing, and personal data shall be collected and processed fairly and in a transparent manner.

The Company ensures that the data subjects can be identified only for the period necessary for the purpose of processing. The Company processes data while it is necessary for the Company's purposes, and closely monitors the retention period, at the end of which performs the activities required for erasure and/or anonymization.

It is the interest of the Company to ensure, throughout the duration of processing, the accuracy and the update of data subject to the purpose of processing. However, as the Company collects data that data subjects provide for it voluntarily, the update of the data is beyond the Company's control. Mimox. Kft. ensures that data subjects may be identified as long as it is necessary for the purpose of processing only. Therefore, the Company shall make efforts to call the attention of the data subjects to the periodic update of their data, but data update can only be performed with the voluntary cooperation of the data subjects.

The Company ensures that data can only be accessed by employees or processors whose access is justifiable regarding processing.

Personal data maintains its capacity during processing as long as its relationship with the data subject can be restored. Relationship with the data subject can be restored if the Company possesses the technological means and prerequisites that are necessary for restoration.

I/1 Laws, Recommendations, and Guidelines

This Policy is designed based on and in accordance with the laws, recommendations, policies and internal rules listed below:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Article VI of the Fundamental Law of Hungary
- Act CXII of 2011 on information self-determination and freedom of information ("Info Act")
- Act V of 2013 on Civil Code
- Act CXXXIII of 2005 on the rules of personal and property security and private investigation activities
- Act I of 2012 on labor code ("Labor Code")
- Act C of 2003 on electronic communication
- Act CLV of 1997 on consumer protection
- published recommendation of the Hungarian National Authority for Data Protection and Freedom of Information

II Scope and Responsibilities

II/1 Personal Scope

The personal scope of this Policy covers the organizational units and employees of the Company as well as the persons, legal entities and other organizations that sign contracts with the Company to the extent defined in those contracts or the respective confidentiality agreements.

II/2 Material Scope

The material scope of this Policy covers any processing performed at any organizational unit of the Company that handles personal data, whether or not processing is performed manually or by partly or fully automated means.

II/3 Update of Policy

The internal data protection officer ("data protection manager") of the Company is responsible for the compilation and update, as necessary, of this Policy.

III Data Protection Officer

The data protection officer of Mimox Kft is Ms. Csudinka Csudutov, the managing director of the Company. Her phone number is +36209606731; her email address is csudi@mimox.com. As per applicable laws, her consent is not required for the display of those pieces of information. Nonetheless, she gives her consent to their display.

IV Data Controllers

The controllers at Mimox Kft. are the employees of the Company whose position is "counsellor." The employees of the Company may transfer personal data internally to counsellor employees of the Company only. As of April 16, 2019, those persons are as follows:

- Ágota Berend
- Csudinka Csudutov
- Blanka Marton
- Zsuzsanna Schleer
- Ádám Toldi

V Employee Data

V/1 Legal Basis of Processing

Processing is required in order to fulfil the legal requirements of the controller. Such data are the names of the employees, the names of their mothers, the numbers of their bank accounts, their tax IDs, the numbers of their ID cards, their social insurance numbers, the dates of their hire and termination, and the information on the statements they received from their former employers.

Data regarding the number of their children, the names and tax IDs of their children, the names of the other parents or guardians of their children as well as the names of the employers of the

other parents or guardians of their children shall also be collected for the purposes of annual leaves and family tax benefits.

Those employee data may be accessed by the data protection manager or the data processor of Mimox Kft.

V/2 Data Processor

The data processor of Mimox Kft. is Econoserve Gazdasági Tanácsadó Kft. (address: Apt. 103, 1st floor, 7/A Szerémi út, Budapest, 1117; tax ID: 10657744-2-43, bank account number: 12010855-01555999-00100006) and/or its subcontractors, which is/are responsible for the accounting and payroll tasks for the Company.

V/3 Monitoring Employees

The associates of Mimox Kft. may work according to flexible work schedules from any places of their choosing because the infrastructure solution applied by the Company enables them to do so. That means that they may work from anywhere with internet access, even from home. Therefore, Mimox Kft. does not monitor its employees in any way regarding the way, the time when and the place where they work.

Mimox Kft. provides its associates with electronic tools (such as computers or notebooks and mobile phones with software installed) for their work, and the associates are allowed to use those devices for their personal purposes as well. IT security is, however, checked on those devices in an ad hoc manner, even without prior notification of the affected employees. The data protection manager may collect the computers or the mobile phones from the employees to perform full system updates, and the data protection manager may delete any data from those devices.

The employees of Mimox Kft. are responsible for saving their personal documents periodically on another device not owned by Mimox Kft. or using a cloud service provider to the extent they use the devices for their personal purposes.

As Windows operating systems run on the notebooks of Mimox Kft., Mimox Kft. informs its employees about Microsoft's privacy policy and methods of data collection, and requires them to read the following documents:

https://privacy.microsoft.com/en-us/privacystatement or https://privacy.microsoft.com/hu-hu/windows10privacy and https://privacy.microsoft.com/hu-hu/privacystatement

V/4 When Is Checking of IT Devices Justified

- When an employee discloses any information to be protected and which was obtained during the performance of his or her duties in connection with his or her job to any unauthorized person or organization.
- When an employee fails to comply with his or her obligation for cooperation with his or her employer.
- When it is impossible to obtain consent from the data subject employee and it is requested by his or her relative in writing with specifying the reasons for the request, and it is reasonable to assume that the disclosure of personal data is necessary for the protection of vital interests of the data subject employee, and the disclosure of personal data is deemed to be justified and proportional with the right of informational self-determination by the data protection manager.

- Any circumstances that render it reasonable to assume that an employee has materially violated any general ethical standards, which is deemed to be justified and proportional with the right of informational self-determination by the data protection manager

V/5 General Confidentiality Directives for Employees

The employees of Mimox Kft. agreed to the following terms in their employment contracts:

"7.1. Employee shall handle any technical, financial, legal or other data or information regarding Employer, the Employer's group of companies, the products, services, employees, agents, business partners, etc. of Employer and obtained during his or her employment from Employer or any third party having contractual relationship with Employer or any third party that has confidentiality obligation towards Employer. Employee shall not disclose such data or information to third parties, use or publish otherwise such data or information in any way without prior written permission of Employer. The confidentiality obligation of Employee remains in full force and effect after the termination of this Employment Contract.

"7.2. Employee shall implement any reasonable measures necessary to prevent unauthorized access to the information constituting the subject matter of the confidentiality obligation, and shall ensure adequate and secure storage of such information, in particular that of information stored on electronic devices, mobile phones or computers.

"7.3. Should Employee violate this confidentiality obligation, Employer may terminate this Employment Contract immediately. Employee shall be responsible for any and all losses arising out of his or her violation of the confidentiality obligation."

VI Customer Data

The business partners of Mimox Kft. are mainly legal entities that order its services. For persons, Mimox Kft. asks for and uses personal data that are necessary to create invoices only; such invoices are created for a training for job interviews in English.

Mimox Kft. does not send marketing newsletters or collect email addresses for marketing purposes.

Mimox Kft. does not provide services to customers that need their access to personal data. Therefore, Mimox Kft. does not possess any personal data the loss of which could cause any damage to any of its customers. As a consequence, there is no need to be prepared for the timely restoration of access to and availability of personal data in the case of a physical or technical incident, because there is nothing to restore.

The employees of Mimox Kft. may contact the employees of customers, and while conducting business activities, they may obtain email addresses and work phone numbers of certain employees of customers or information regarding the work schedules of such employees of customers; the vast majority of such information can be found in the mailing system of Mimox Kft.

As per applicable laws, any business, including Mimox Kft., shall obtain a consent for processing from the persons (representatives, contact persons, etc.) who are named in a contract entered into with a legal entity or other organization; therefore, Mimox Kft. provides separate section for such a consent in its contracts.

VII Data for Persons Applied for Carrier Counselling or Posted Positions/Jobs (“Candidates”)

VII/1 Purpose of Collection

The purpose of Mimox Kft.'s request for the CVs and contact details of the candidates (those who are looking for jobs) is to enable the Company to communicate with and make appointments and offer carrier opportunities for the candidates. It is also the purpose of the collection of such information to enable the associates of Mimox Kft. to improve the CVs or suggest improvements to the CVs in order to facilitate finding jobs for the candidates, increase the number of candidates called in for job interviews relative to the number of applicants, and help the candidates be aware of their strengths and capabilities so that they be able to build their carriers more efficiently.

VII/2 Legal Basis of Processing

The Company shall not process personal data without the consent of the data subjects.

VII/3 Method of Collection

The candidates upload their CVs via the website of Mimox Kft. or send them via email to the associates of the Company or might share their documents via social media platforms voluntarily. When uploading via the website, the candidates need to read and accept the privacy and data processing policy of Mimox Kft. Those sending their personal data via emails or other means, however, are required to subsequently learn that policy and indicate acceptance.

Mimox Kft. organizes face-to-face or online (such as via Skype) meetings with certain but not necessarily each candidate, during which it collects information regarding the carrier plans, prior professional experiences, compensation expectation, current salary, professional impression, or other personal circumstances of the candidate that the candidate may share voluntarily with the counsellor employee. Mimox Kft. may create candidate profiles from those pieces of information so that it be able to offer the best carrier opportunity for the candidate.

With full knowledge and consent of the candidate, Mimox Kft. may initiate reference interviews with former colleagues of the candidates.

Mimox Kft. retains the submitted CVs, the provided contact details and the information collected during the personal interview and the reference interviews for two years; then it erases them from its systems unless a new informed consent is received from the data subject candidate.

VII/4 Implementing Purpose Limitation

It is always the task and responsibility of the processing associates to check whether the principle of purpose limitation is implemented. When handling requests for disclosure, when handling customer requests for candidate personal data disclosure in particular, the processing associate shall always judge whether the data requested is essential for the purpose specified in the request (such as suitability for a position or disclosure of a job offer). The requestor may only be provided with personal data that is essential for that purpose. If the purpose limitation of processing is questionable, the personal data manager shall seek the opinion of the data protection manager.

VII/5 Physical Conditions of Face-To-Face Meetings

When candidates participate face-to-face meetings, they, typically but not exclusively, meet associates of Mimox Kft. in the offices of Mimox Kft. at 76 Váci út, Budapest, 1133. To the best knowledge of Mimox Kft., there are no surveillance cameras in the building, which is operated by CA IMMO Real Estate Management Hungary Kft. Should there be any surveillance cameras in the building, recordings made by them are solely available for the building operation company and any processing is their responsibility.

The CVs of those attending carries counselling are printed and commented for the purpose of helping the counsellor analyze the carrier path and interpretation of professional projects. Moreover, those comments visualize the steps necessary of restructuring the document for the benefit of the candidate. The printed and commented document is scanned and transferred to the mailing system of the Company as electronic data via Epson Connect[1]. It is subsequently copied to the online data storage of Mimox Kft. The original paper document is shredded within one week after the date of carrier counselling to make it unavailable and inaccessible. The document shredder is owned by First Clients Capital Square Kft. and is located in the common area of the offices serviced.

VII/6 Special (Sensitive) Personal Data

The Company may process special personal data only if the data subject provides explicit consent for doing so. If a candidate indicates his or her handicap voluntarily, either orally or in writing, that information is transferred to the potential employers only if it is essential for the provision of the conditions of work and only if the candidate agrees and requests such a transfer. If a candidate does not disclose information regarding his or her handicap to the Company, the Company makes no attempt to reveal such characteristics or any other special personal data.

VII/7 Access to Personal Data

No candidate or client has any access to his or her own or other persons' personal data stored by Mimox Kft.; they are not provided with any paths for that purpose; that enables them to access, store, or update such data from any web browser.

Mimox Kft. is using the applicant tracking system (ATS) with two-factor authentication provided by HR Szoftver Kft. (address: 2045, Törökbálint, Kossuth Lajos utca 40., Hungary, Co. registration No.: 13-09-190859, VAT No: 14433070-2-13), available at ats.mimox.info. Data protection in the ATS is guaranteed by HR Szoftver Kft.

The persons (candidates) who wish to receive copies of personal data the Company possesses on them may request copies of those personal data via the mimoxprivacy@mimox.com email address with a subject line of “request for personal data” (“adatot kérek”). The Company shall respond to such requests within 8 calendar days.

[1] Epson' Privacy Statement guarantees that Seiko Epson Corporation does not store copies of transferred documents on its servers. (Printing Solutions Operations Division, 80 Harashinden, Hirooka, Shiojiri, Nagano-ken, Japan; email: privacy.epsonconnect@exc.epson.co.jp)

VII/8 Data Transfer to Third Countries

Mimox Kft. transfers the personal data of the candidates into countries outside of the European Union in exceptional cases only, typically into an applicant tracking system (ATS) operated in the United States and used by the customers of Mimox Kft. Greenhouse or Lever are examples for such systems.

VII/9 Requests for Ceasing of Processing

The persons who wish the Company cease the processing of their personal data, that is, erase the information stored regarding them, may request erasure via the mimoxprivacy@mimox.com email address with a subject line of "request for erasure" ("törlést kérek"). The Company shall respond to such requests within 8 calendar days.

VIII Data Processing and Privacy Clauses of the Information Security Policy of Mimox Kft.

Mimox Kft. requires that its employees always act with utmost diligence and foresight.

VIII/1 Maintenance of Computers, Notebooks, and Mobile Devices

Mimox Kft. provides its associates with computers and notebooks with virus scanner and local firewall software installed. The associates are responsible for periodically downloading and installing all updates for the operating system, the virus scanner and other software they use. Those updates are checked by the data protection manager with no prior notice.

The associates of Mimox Kft. may not assign, either temporarily or permanently, the hardware devices owned by Mimox Kft. to anyone not employed by Mimox Kft., and may not leave them unattended any time. In case they do not have those devices on them, they shall ensure that those devices are stored in a locked room that is not accessible by anyone else.

VIII/2 Passwords

Any hardware device used by the associates shall be password protected.

The associates may not use identical passwords for different systems, and they shall change the passwords periodically. The strength of the passwords shall meet the software requirements of the different systems.

On the state-of-the art notebooks used by Mimox Kft., users shall be authenticated at login using the iris pattern recognition or finger print recognition feature.

VIII/3 User Privileges

The data protection manager has administrative privileges, while each other employee of Mimox Kft. has user privileges in all online systems used by the Company. The associates have administrative privileges on all the electronic devices provided for them by Mimox Kft., such as their notebooks and mobile phones. An administrator profile shall be separated on each of their computers, which shall be used by the associate with a user profile during their daily work.

VIII/4 Storing Data Electronically

The employees of Mimox Kft. may save and store any data related to their work on online data storage provided by Mimox Kft. No data that is subject to any confidentiality obligations or contains any personal data may be stored on personal computers, notebooks, or mobile phones, with the exception of temporary storage of technical nature, such as local opening or editing of a document physically residing on a remote server. The employees shall periodically erase such data from their devices. Such erasures shall be periodically checked by the data protection manager of Mimox Kft., who may collect the hardware devices from the associates for the purposes of performing such checks.

The company permits the personal use of its hardware devices, but any employee shall ensure that his or her personal data are not stored on the devices of the Company permanently. The data protection manager may instruct that all data and software be completely erased from the devices owned by the Company if he or she finds that data protection cannot be ensured otherwise. (See also section “What to Do in the Case of Hardware Malfunction.”)

VIII/5 Backups

The data protection manager shall make weekly or monthly backups of the content of the file server for the sole purpose of enabling the restoration of the files accidentally deleted. The content of the database and that of the mailing system need no separate backup as the cloud service provider (MS Azure and MS O365) makes backups automatically, and those backups may be used for restoration in the case of accidental or inappropriate change of some data. (The built-in service of the systems is the option for restoring a previous state by specifying a period of time.)

VIII/6 Other Data Protection Measures

On the devices used by the associates, it is required to set up the built-in smart IT solutions that enable finding the device: “Find My Device” (Android), “Find My iPhone” (iOS), or “Find My Device” (Windows 10).

IX Storing Data on Paper

Mimox Kft. stores paper documents in its registered offices. Data may be processed by the counsellor associates of the Company or the data processor of the Company.

Mimox Kft. does not store paper documents regarding candidates, unless for a temporary period specified in paragraph VII/5 above before the paper documents are physically destroyed. The associates shall ensure that no personal data of any candidate, such as CV, proof of degree, or interview records, ever remain at any place visible.

X Data Protection Performance Tests and Vulnerability

X/1 Media

It means vulnerability for Mimox Kft. if any electronic devices or media in the possession of its associates

- are stolen by a third party
- are lost
- render their passwords available by a third party
- are being repaired due to hardware malfunction

X/2 Storing Data

Mimox Kft. stores personal data usign cloud service providers or, temporarily, on notebooks and mobile phones in the possession of its associates. The cloud service providers used are Jungle Disk Llc. and Microsoft, Inc. Mimox Kft. does not have any self-hosted computer network or servers.

X/2.1. Jungle Disk

The address of the company is: 110 E Houston St., Ste. 209, San Antonio, TX 78205, USA

Its privacy policy is available at: https://www.jungledisk.com/privacy/
email: privacy@jungledisk.com

Its security practices are available at: https://www.jungledisk.com/security-practices/

Data stored on the servers of Jungle DIsk are encrypted using AES-256. Jungle Disk does not store the passwords of Mimox Kft. Once the passwords are lost, the data become inaccessible, which may cause business loss for Mimox Kft., but will not make any personal data of third parties or employees available for any unauthorized persons. The master passwords are known only by the data protection manager.

X/2.2. Microsoft Azure

The address of the company is: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA

Its privacy statement is available at: https://privacy.microsoft.com/hu-hu/privacystatement#mainnoticetoendusersmodule

While using O365 and MS Azure services, Mimox Kft. respects and follows Microsoft's recommendations for privacy.

X/3 Transferring Data

There are two methods for transferring data. One method uses our website (https://mimox.com), where the candidates upload their names, phone numbers, email addresses and CVs, and the other method means sending the CVs of the candidates to other associates of the Company or its customers via our email systems.

Security of the data transfer via the website is ensured by our vendor, Lajos Levente Rácz, private entrepreneur (registration number: 50432181; principal place of business: Apt. 2, ground floor, 15 Géresi utca, Debrecen, 4028; tax ID: 58911648-1.29).

It may generate vulnerability when our associates transfer documents containing personal data to incorrect email addresses.

X/4 Former Employees

Further handling and use of personal data that might be stored on electronic devices owned by former employees may also mean vulnerability. Copies of such personal data might have been stored on the devices of former employees before the effective date of this data processing Policy. Mimox Kft. is not responsible for the processing of such copies.

X/5 Offices

First Clients Capital Square Kft. (address: 76 Váci út, Budapest, 1133, tax ID: 14509021-2-41.) provides coworking offices and business address services to Mimox Kft.

X/6 When the Data Protection Manager Dies

If the data protection manager dies, Mimox Kft. will have no access to the backups of its candidate databases, business documents, and mailing system, and Mimox Kft. cannot configure the systems or change the passwords with the exception of the passwords of the Company's mailings system, to which Ádám Toldi and Ágota Berend has administrative privileges. Though the occurrence of such an incident significantly violates the business interests of Mimox Kft., neither employees, nor candidates will experience any damage as far as the processing of their personal data is concerned.

XI Handling of Personal Data Breaches

Should an IT media be stolen, lost, or damaged, the associates of Mimox Kft. shall immediately notify the data protection manager or, simultaneously, any other associate via email, telephone, text message (SMS), or in person if the former methods are not available or the notification attempt failed. When such a personal data breach occurs, the associates shall notify the data protection manager regardless of his or her current activities or time of day.

XI/1 Records of Personal Data Breaches

Personal data breaches are recorded in the *adatvedelmiIncidensNyilvantartas.xlsx* file in the specified directory on the file server of the Company.

The records of personal data breaches contain the facts related to the personal data breach: the time it probably happened, the time it was noticed, description of the incident (facts and circumstances), description of the affected data subjects, the kind of personal data involved in the personal data breach, cause of the personal data breach, effects of the personal data breach (possible risks and consequences), description of remedies implemented, reasons for the actual measures and their effects.

XI/2 What to Do in Case Media is Stolen or Lost

Should such a personal data breach occur, the data protection manager shall immediately change the passwords in the central IT systems of the Company, namely in the G4 software, the Jungle Disk storage and the O365 mailing and filing system.

Then the data protection manager shall:

- record the personal data breach
- report the personal data breach to the data protection authorities within 24 hours
- notify the applicable investigating authorities in case of a willful or supposedly willful appropriation
- if it is possible, notify the data subject(s) and inform them on their personal data involved in the personal data breach

When those measures are implemented, the Company attempts to track or recover the storage device using the smart IT solutions offered by the operating systems on the devices: “Find My Phone” (Android), “Find My iPhone” (iOS), or “Find My Device” (Windows 10).

XI/3 What to Do in the Case of Hardware Malfunction

If a piece of hardware needs servicing, the following software shall be deleted from the device before it is taken to the service center for repair wherever it is possible, that is, wherever the media is accessible via software:

- Jungle Disk Workgroup
- G4

The following items shall also be deleted:

- complete profile(s) of user(s)
- browsing history folder(s) of browser(s)
- deleted items folders

The data protection manager shall generate a new password for the user using that computer in the G4 software, the Jungle Disk storage and the O365 mailing and filing system.

With those measures implemented, the risk of obtaining personal data by unauthorized persons is reduced to minimum, because the restoration of the data deleted from the media is possible in

a laboratory environment and in theory only. Thus, basically, a device with a blank new user profile is provided.

If data are inaccessible on the malfunctioning piece of hardware, the data protection manager shall ensure that the media (storage or memory card) be removed and destroyed, that is, made permanently unusable. (As for the hardware device without that media, Mimox Kft. applies separate collection scheme for disposing, or donates it for educational purposes)

XI/4 What to Do in the Case of Unauthorized Intrusion to the Offices

Should an unauthorized person intrude into the offices of Mimox Kft., the data protection manager shall:

- record the personal data breach
- notify the applicable investigating authorities
- report the personal data breach to the data protection authorities within 24 hours if it is possible or likely that the intruder obtained personal data
- notify the data subject(s) and inform them which of their personal data are involved in the personal data breach

XI/5 Data Transfer to an Incorrect Email Address

Should such a personal data breach occur, the owner of the used incorrect email address shall be notified immediately that he or she is not eligible to read the content of the email and shall be asked to delete that email. The data protection manager shall also be notified immediately, who in turn shall enter the personal data breach into the relevant recording system. The data protection manager shall notify the data subjects as well if needed.

XI/6 Reporting Personal Data Breaches

Should a personal data breach occur, Mimox Kft. reports it to the Hungarian National Authority for Data Protection and Freedom of Information (email: http://www.naih.hu; address: 22/C Szilágyi Erzsébet fasor, Budapest, 1125; phone +3613911400).

XII Records on Data Processing Activities

Name and address of controller: Mimox Kft, 76 Váci út, Budapest, 1133

Data protection manager or officer: Ms. Csudinka Csudutov; phone: +36 20 9606731; email: csudi@mimox.com

Purposes and legal basis of processing: Processing personal data of the employees of Mimox Kft. to execute employment contracts or meet legal requirements. Processing of personal data of the customers and candidates of Mimox Kft. for the purposes of its legitimate interests, where the legal basis of processing is the consent of the data subjects.

Categories of personal data processed by Mimox Kft.: Name, phone number, residential address, email address, photo, date of birth, qualifications, former employers, interests, payment details. For employees, the following personal data are also processed: place of birth, social insurance number, tax ID, bank account number, number of ID card, name of the mother of the employee, name(s), tax ID(s), and date(s) and place(s) of birth of the child (children) of the employee.

Categories of recipients: Organizations with which Mimox Kft. makes business or signs contracts, where Mimox Kft. is the vendor.

Personal data may be transferred or repeatedly transferred to third countries or international organizations only with the consent of the data subject and after informing the data subject that organizations located outside of the countries of the EU are not obliged to meet the terms of GDPR. Such transfer is permitted only if it is between Mimox Kft. and its customers and required for the execution of a contract for the benefit of the data subject.

Schedule for the erasure of personal data: For employees, it is the time specified by the applicable laws; for candidates, it is two years from the date of the candidate's consent, in all categories.

Data processor of Mimox Kft.: Econoserve Gazdasági Tanácsadó Kft. and/or its subcontractors (address: Apt. 103, 1st floor, 7/A Szerémi út, Budapest, 1117; tax ID: 10657744-2-43; bank account number: 12010855-01555999-00100006). Category of data processing: accounting and payroll.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Mimox Kft. and Econoserve Gazdasági Tanácsadó Kft. shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. They shall ensure the confidentiality, integrity, availability and robustness of the systems and services used to process personal data. For employee data, they shall ensure via continuous and safe data storage and backups that in case of a physical or technical incident, they be capable for timely restore of access and availability of the employees' personal data. Mimox Kft. shall test, assess and evaluate the technical and organizational measures implemented to guarantee the safety of processing.

XIIIDefinitions

For the purposes of this Policy and in accordance with the applicable laws, the terms defined below are used:

Data is a sequence of signs or primitives represented in a system that have meaning or sense, or may refer to or describe something. The complete information data represents is determined by its environment. Therefore, data is information without meaning.

Data file or **file** means the set of data on records.

Database means an organized collection of data handled by a software for storing, retrieving and editing data. An essential feature of a database is that it stores data as well as relations among data. A database is not a database management system, which is a software (program) for operating a database and organizing system and user processes.

Group of data refers to data (that is a formalized display of facts, concepts or instructions, a fixed sequence of signs, disclosure via voice or technological means, for interpretation and processing purposes; for the purposes of this Policy, it is any text, sequence of numbers, facts, information, designs, charts, pictures, or illustrations created in writing or electronically and stored on any media) and categories, usually based on a filing function.

Data safety is a state of an IT (data storage and processing) system in which the risk of losing or destroying data can be reduced to acceptable level by appropriate means. That state is achieved by following regulations and precautions based on international standards related to the integrity and reliability of information.

Data processing is the performance of the technical tasks related to processing, regardless of the methods or tools used for the performance of those tasks as well as the location of the application, provided the tasks are performed on the data.

Processor means a person or legal entity or other organization that processes data on a contractual basis, including, without limitation, contracts signed by law.

Media means the physical form and place of storage of data, including data itself.

Processing means any and all operations performed on data, irrespective of the method used, such as collection, recording, organization, storage, adaptation or alteration, use, retrieval, disclosure, alignment or combination, locking, erasure or destruction as well as prevention of further use of data, making photo, voice or video recording, and recording personally identifiable information (such as finger print, palm print, DNA sample or iris pattern).

Restriction of processing means the marking of the stored personal data with the aim of limiting their processing in the future.

Controller means the person or legal entity or other organization which, alone or jointly with others, determines the purposes of processing, makes decisions regarding processing (including the means to use) and performs or has the processor perform such decisions.

Category means a set of named data types or business data functionally related to one another from usage perspective. It is a set that can and should be handled uniformly at logic level and the elements of which needs nearly the same level of protection (such as cashier data, cash data, or remittance data).

Destruction means the complete physical destruction of the media containing data.

Transfer means making data available for a specified third party.

Erasure means making data unrecognizable so that it cannot be restored.

Marking means adding an identifier to data for the purpose of differentiation.

Privacy means the rules, procedures, means and methods of processing that ensure lawful processing of personal data and protection of data subjects.

Personal data breach means the unlawful processing of personal data, such as unauthorized access, alteration, transfer, disclosure, erasure, destruction or accidental destruction or damage.

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Data protection officer means an employee designated by the controller who has sufficient knowledge regarding privacy and takes part in the performance of privacy related tasks.

Locking means the assignment of a mark to data for the purpose of limiting its further processing for a specified period or forever.

Anonymization means a method for making it completely impossible to restore the connection between data and a data subject.

Criminal personal data means personal data that relates to the data subject and is revealed by the authorities that are entitled to perform criminal procedures or discover crimes during or before the criminal procedure, in connection to a crime or a criminal procedure, as well as the personal data revealing criminal records of the data subject.

Cookie means a small data file that is placed by the visited website on the user's computer to facilitate or make more convenient to use the infocommunication or internet-based service. Temporary cookies are placed on the user's computer for a session (such as the authentication for banking over the internet), while permanent cookies (such as the language preferences of a website) remain on the

computer until the user deletes them. For cookies enable the tracking of the user's browsing behavior, cookies may only be placed on the user's device with the permission of the user.

Direct marketing means the information activities and supplemental services utilizing direct connections for the purpose of offering products or services and displaying advertisements for the data subjects or informing trade partners to facilitate making deals (purchases).

Data subject means a person who is identified, directly or indirectly, based on any specific personal data or otherwise. In particular, a person is deemed to be identified if he or she can be identified, directly or indirectly, based on name, ID, or one or more physical, physiological, mental, economic, cultural or social characteristics.

Third party means any person or legal entity or other organization other than the data subject, the controller, or the processor.

Third country means any country that is not a member of EEA (European Economic Area) as per the Info Act.

Consent means the express and explicit expression of the will of a data subject, based on appropriate prior information, which constitutes an unambiguous approval for processing his or her personal data, without limitation or limited to certain actions. With the exception of approval for processing special personal data, consent may be given by an explicit statement or conduct, provided evidence for giving consent is available in any case.

IT tool means any installed or mobile tools created for any task and operated (such as controlled) utilizing information technology as well as any systems, procedures or any components thereof (such as computers, portable IT tools and data storage, printers, operating systems, user applications (office applications, database management systems, firmware, embedded IT systems, and other on-demand custom programs, etc.), IT based telecommunication systems (such as IP phone systems and end devices, active and passive network devices), and components of network management).

Document means a written or electronically created text, series of numbers, design, chart, or picture regarding the operation of an entity or the acts of a person.

Compulsory processing: a law or local government regulation that orders processing determines the types of data to process, the purpose and conditions of processing, the conditions for disclosures, the duration of processing, and the data controller.

Public area means a state or community owned area for public use that can be used as intended by anyone without restrictions, including its parts serving as public roads.

Special personal data: a) personal data revealing skin color, racial or ethnic origin, political opinions or party affiliations, religious or philosophical beliefs, trade union membership, or sex life; and
b) personal data for health status or addiction, and criminal personal data.

Providing adequate information: before processing, the data subject is to be informed whether or not processing is compulsory or based on his or her consent, and the data subject is to be informed in a straightforward manner and in details about any fact regarding the processing his or her personal data, in particular about the purpose and legal basis of processing, the persons eligible for processing, the term of processing and the persons to whom the data may be disclosed. The data subject is to be informed about his or her rights regarding processing as well as his or her remedies.

NAIH stands for Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information). Its status and responsibilities are determined by §38 of the Info Act.

Public data means any facts, data or information that are available to anyone. Only laws may determine whether or not certain personal data should be public.

Disclosure means making data available for anyone.

Personal data means any data that may be connected to a data subject, in particular his or her name, ID, and one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of the data subject, as well as any assumptions derived from the data regarding the data subject. Personal data remain in that capacity during processing as long as its connection to the data subject can be restored, that is as long as the data controller possesses the prerequisites required for restoration.

Personal data manager: For the processing of personal data at a particular organizational unit, personal data manager is the manager of the organizational unit, such as a manager of a store, who is responsible for the processing of any personal data processed by his or her unit to be in accordance with this Policy. If a decision is to be made in connection with any personal data processed in IT systems, and it relates to the responsibilities of the personal data manager, then the personal data manager shall make his or her decision in conjunction with a manager designated in this Policy.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Remote work means any activity performed from outside of the secure zone of the Company's IT system (i.e., from an unsecure environment), during which the Company provides the users with access to IT resources that the user might otherwise have access to at work. It does not mean the ad hoc use of technologies or mobile IT solutions that enable ad hoc communication (such as OWA). For this Policy, meaning of “remote work” is different from that used in the Labor Code.

Objection means any statement made by a data subject for objecting the processing of his or her personal data and requesting the end of processing or the erasure of the processed personal data.

Trade secret means any facts, information or other data, or any combination of them, which relate to the operation of the Company and which are not public or easily accessible for the personnel involved in the operations, and whose retrieval or use by or disclosure to unauthorized persons infringes the legitimate financial, economic or market interests of the Company, provided the Company ensures reasonable protection for its secrets.

Information to protect means any classified data, trade secret, know-how, personal data (restricted handling), any data that is not declared as public or for internal use only, any document prepared for decision making, and any information an employee may learn as part of their job the making available of which for unauthored persons is unlawful, may produce adverse consequences for the employer or any other person, as well as the data processed by the Company whose confidentiality, integrity and availability is among the interests of the Company, unless disclosure is required by law or internal order or the information has already been disclosed by an authorized personnel.

Restricted handling is a general protection protocol for documents containing personal data. If it cannot be clearly identified whether or not the content of a media is to be protected, or if the data controller wishes to emphasize the requirement of restricted handling, the document is to be marked as ”Restricted handling.”